

Internetworking With CISCO Switches



Course Outline

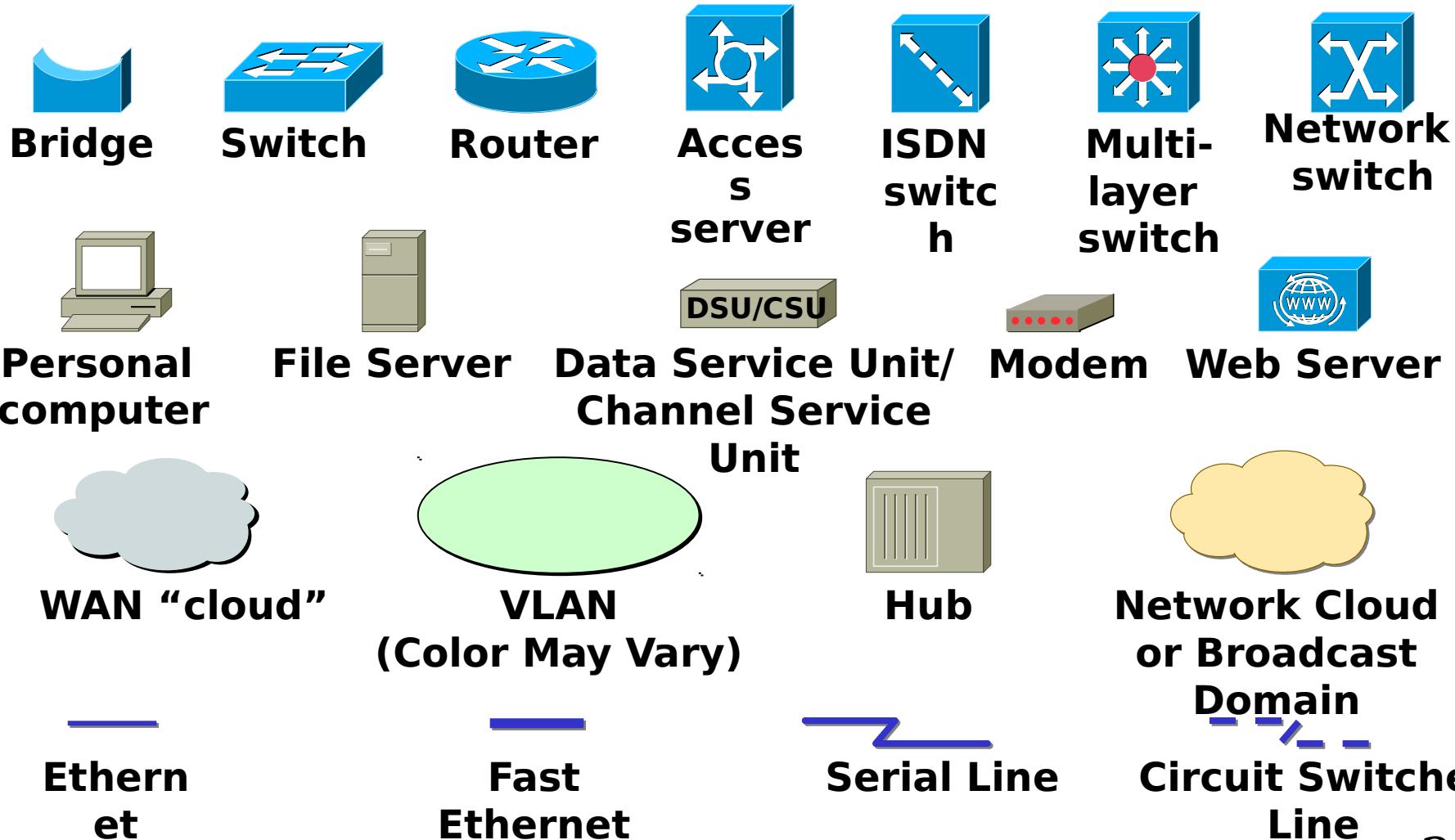
MSTP

- Overview of a Campus Network
 - Switching Technologies
 - Hierarchical Model
 - The Building Block Approach
- Connecting the Switch Block
- Common Workgroups with VLANs
 - VLAN Identification
 - VLAN Trunking Protocol
- Managing Redundant Links
 - Spanning-Tree Protocol
- Inter-VLAN Routing

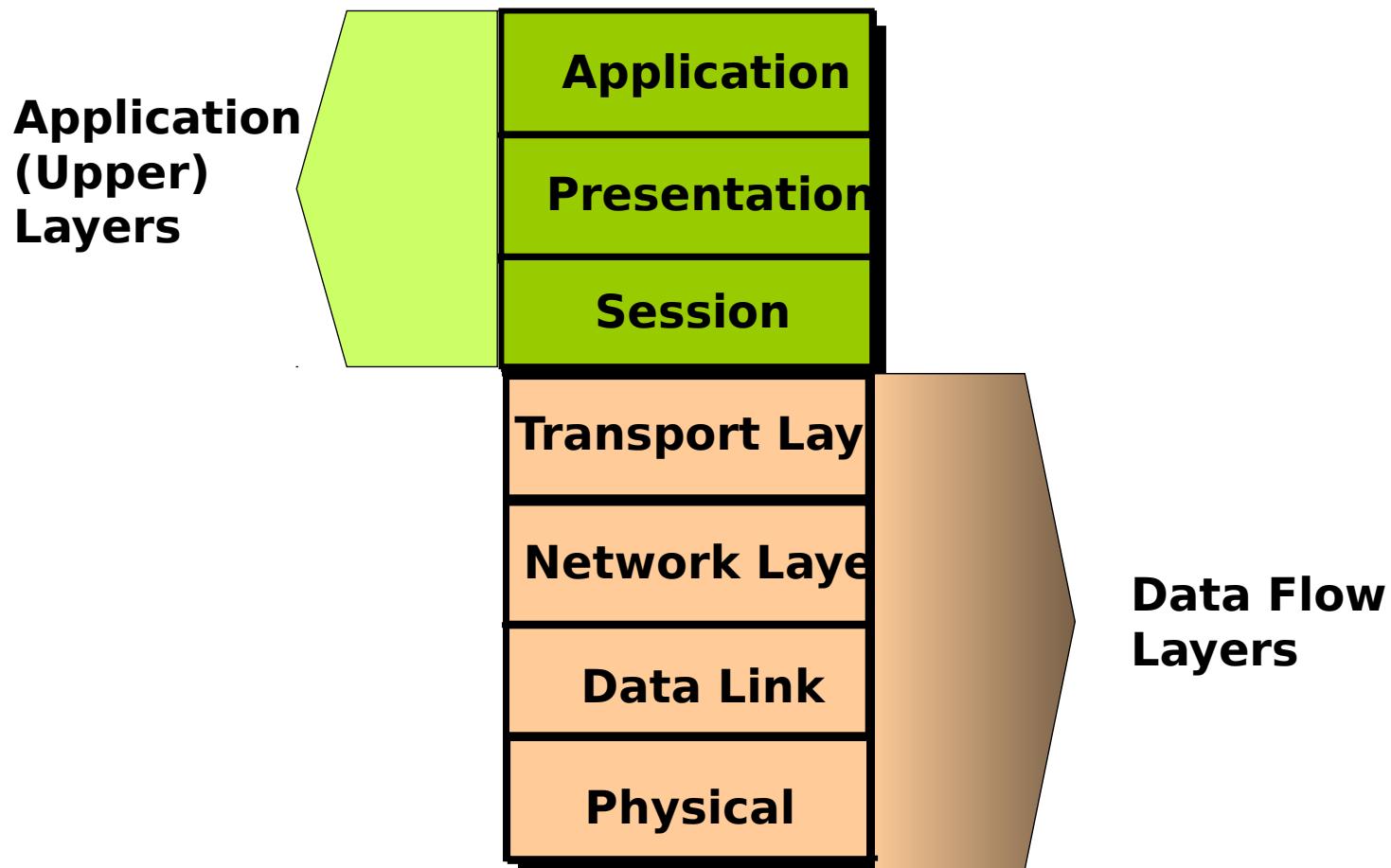


Graphic Symbols

MSTP



OSI Model Overview

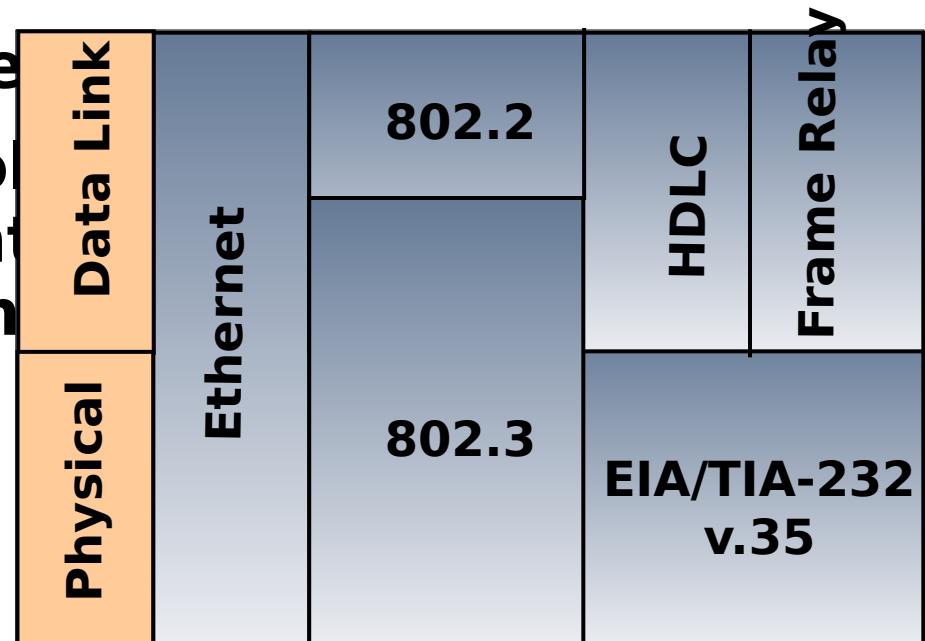


Physical & Data Link Layers

MSTP

Defines

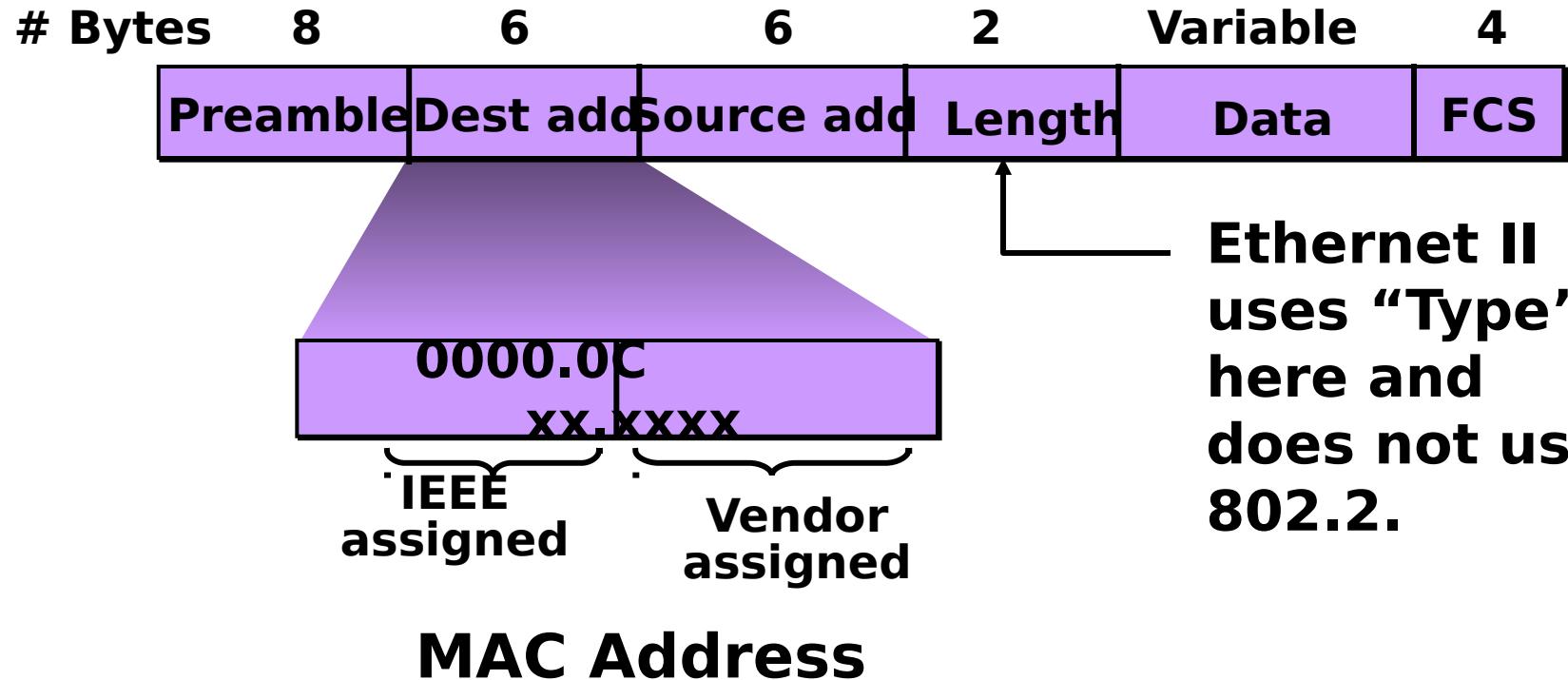
- Physical source and destination addresses
- Higher layer protocols (Service Access Point associated with frame)
- Network topology
- Frame sequencing
- Flow control
- Connection-oriented or connectionless



Data Link Layer

MSTP

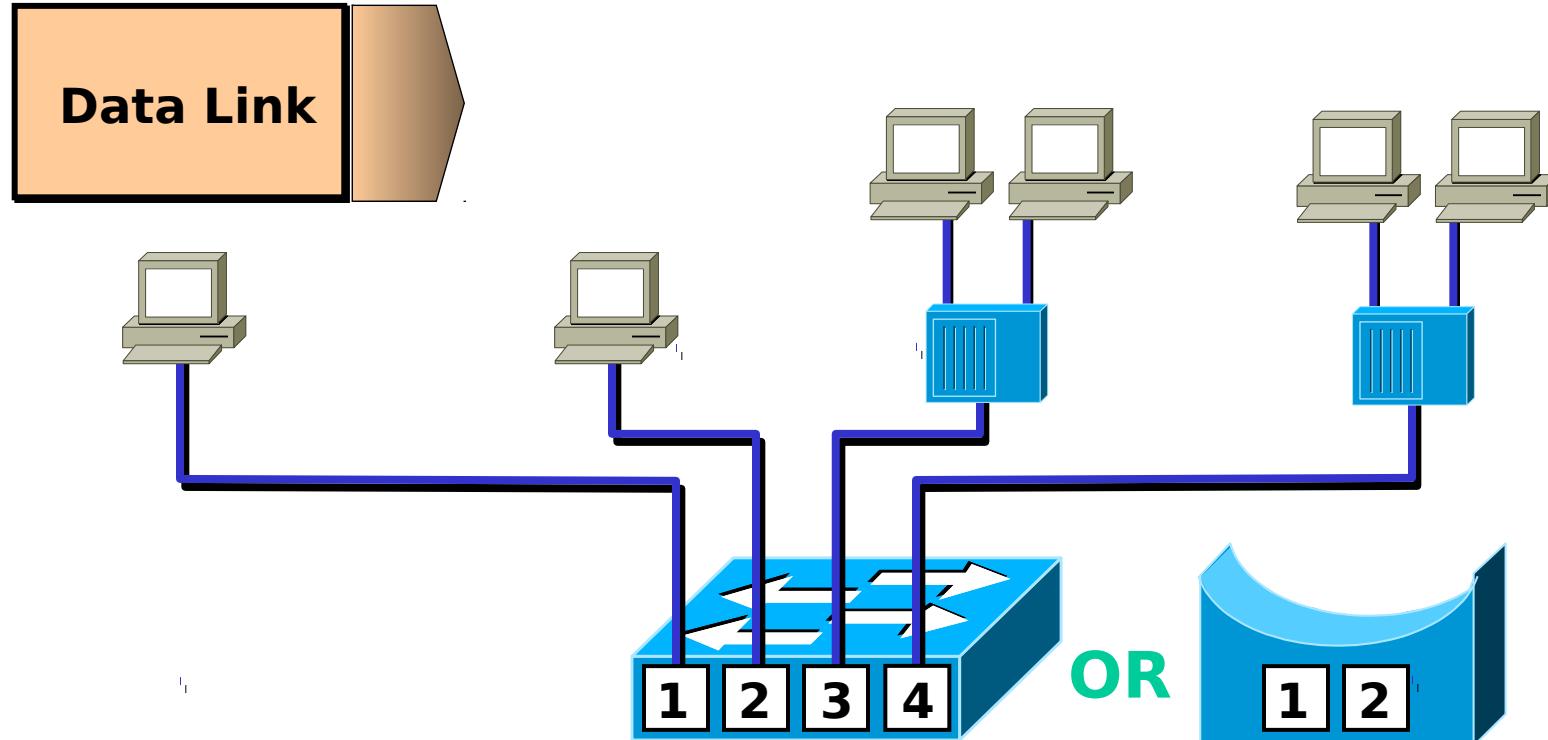
MAC Layer - 802.3



Switches, Bridges, & Hubs



MSTP

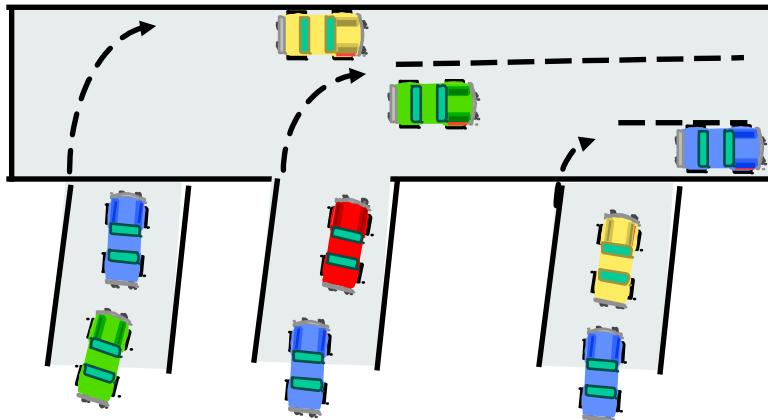


- Each segment has its own collision domain
- All segments are in the same broadcast domain

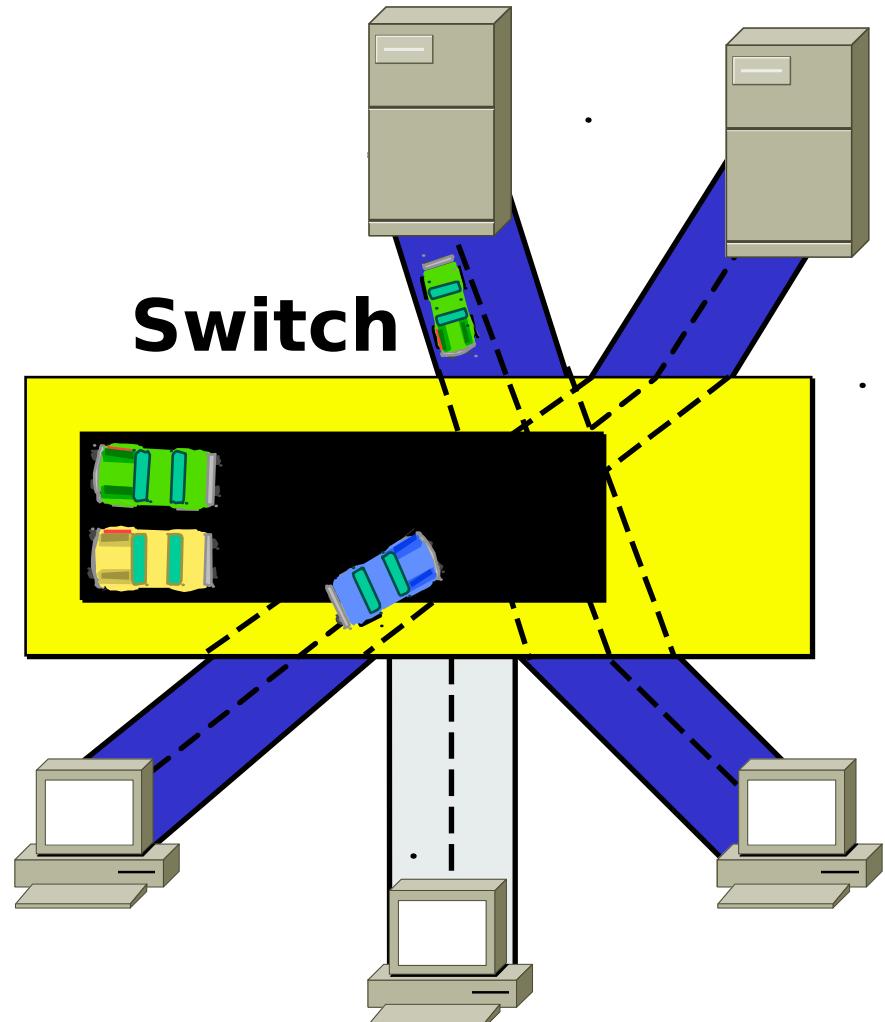
Advantage of Switches



MSTP

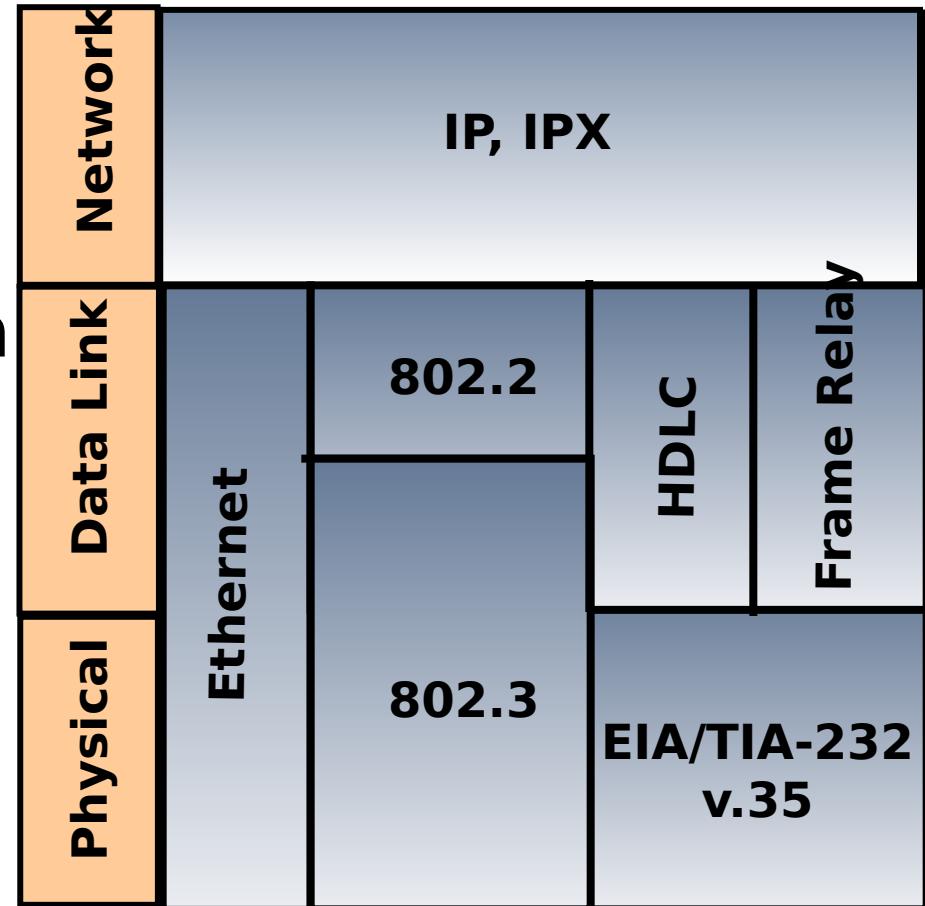


- Each segment has its own collision domain
- Broadcasts are forwarded to all segments

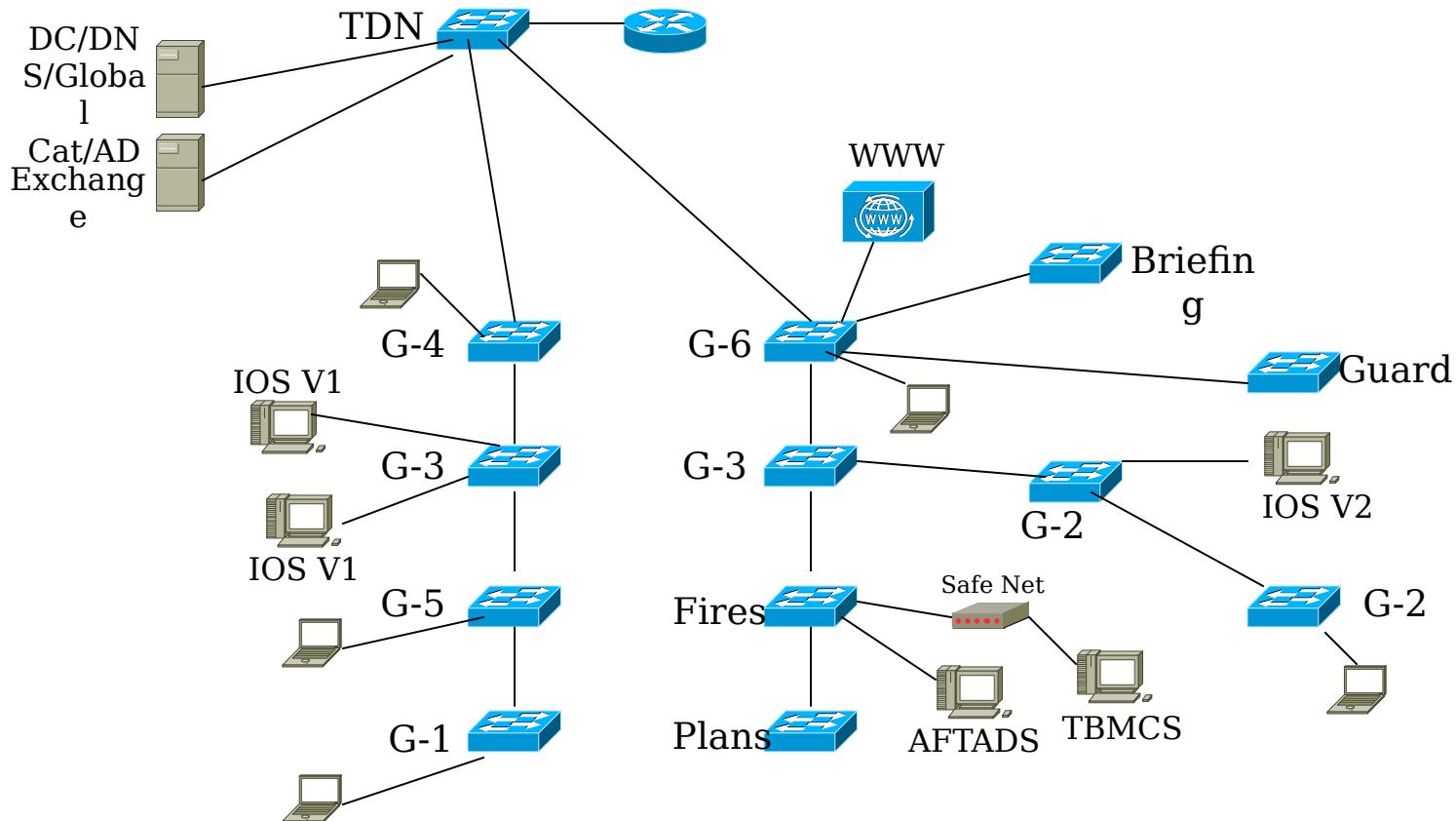


Network Layer Functions

- **Defines logical source and destination addresses associated with a specific protocol**
- **Defines paths through network**
- **Interconnects multiple data links**



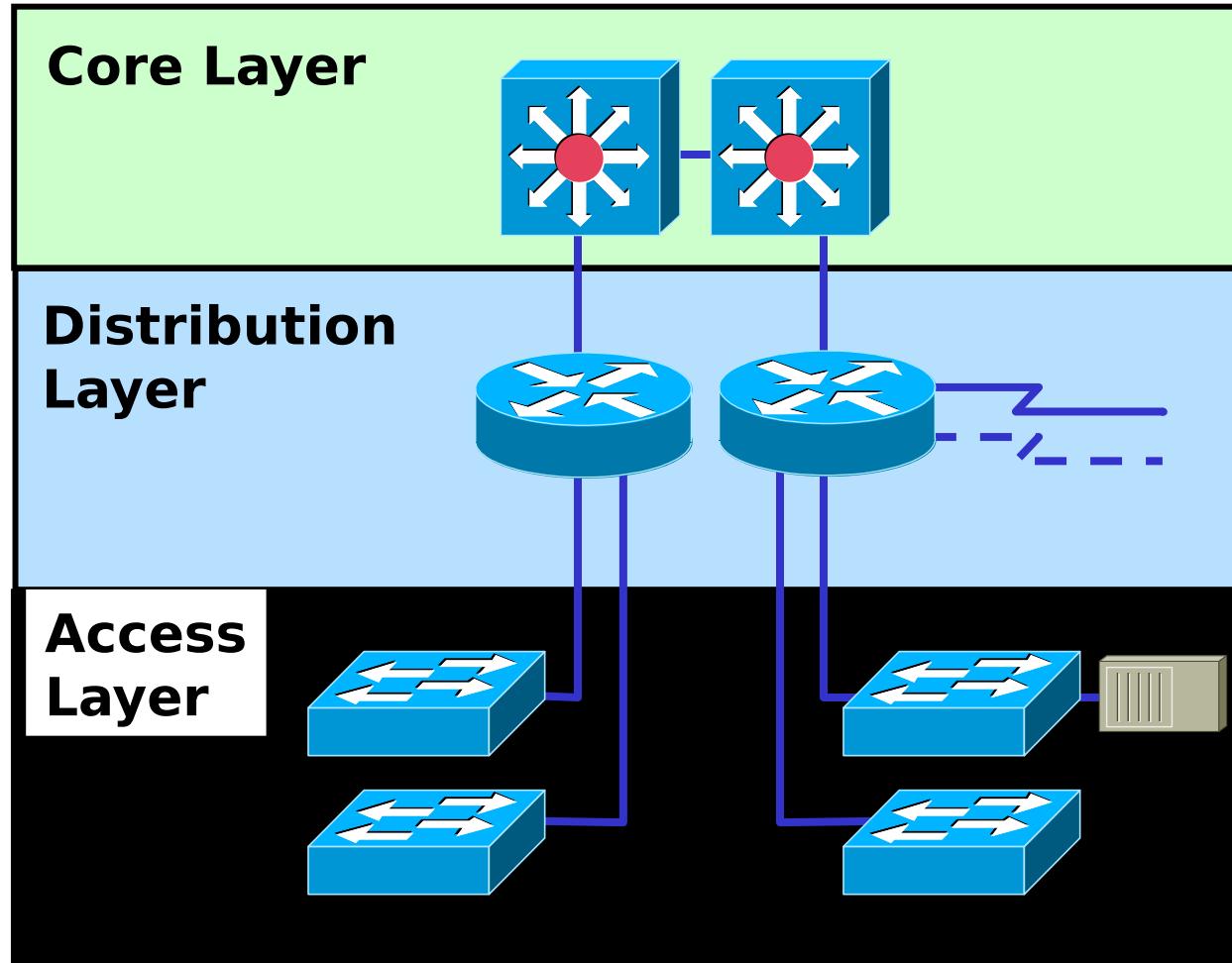
Switching Requirement



Cisco's Network Hierarchy



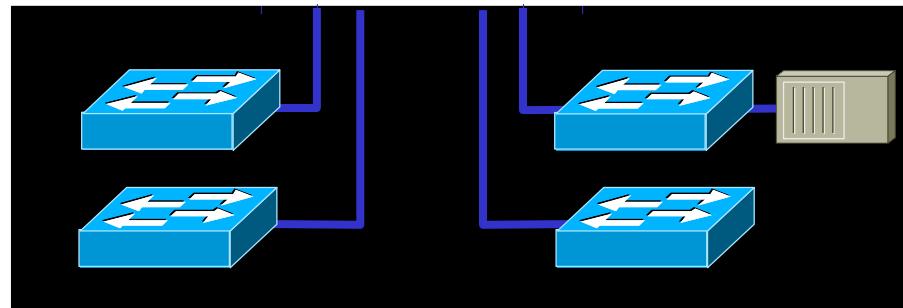
MSTP



Access Layer Characteristics

MSTP

Access Layer



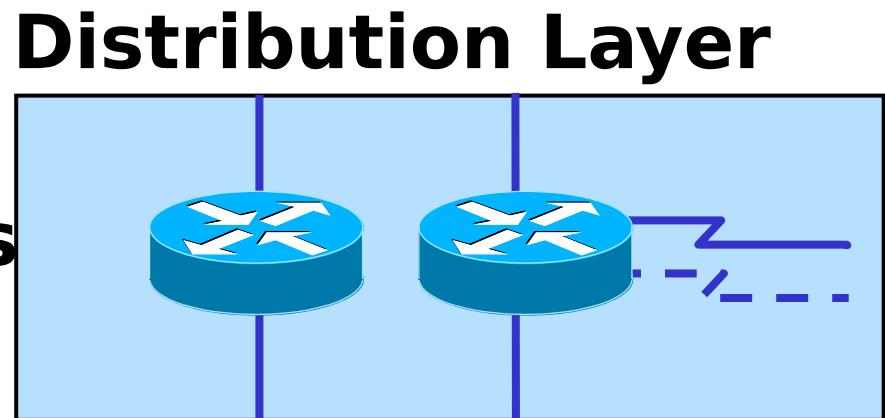
End station entry point to the network

Distribution Layer



MSTP

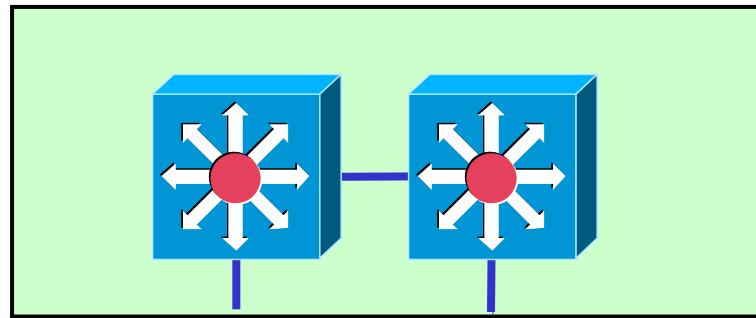
- **Access Layer Aggregation Point**
- **Routes traffic**
- **Broadcast/Multicast Domains**
- **Media Translation**
- **Security**
- **Possible point for remote access**



Core Layer

MSTP

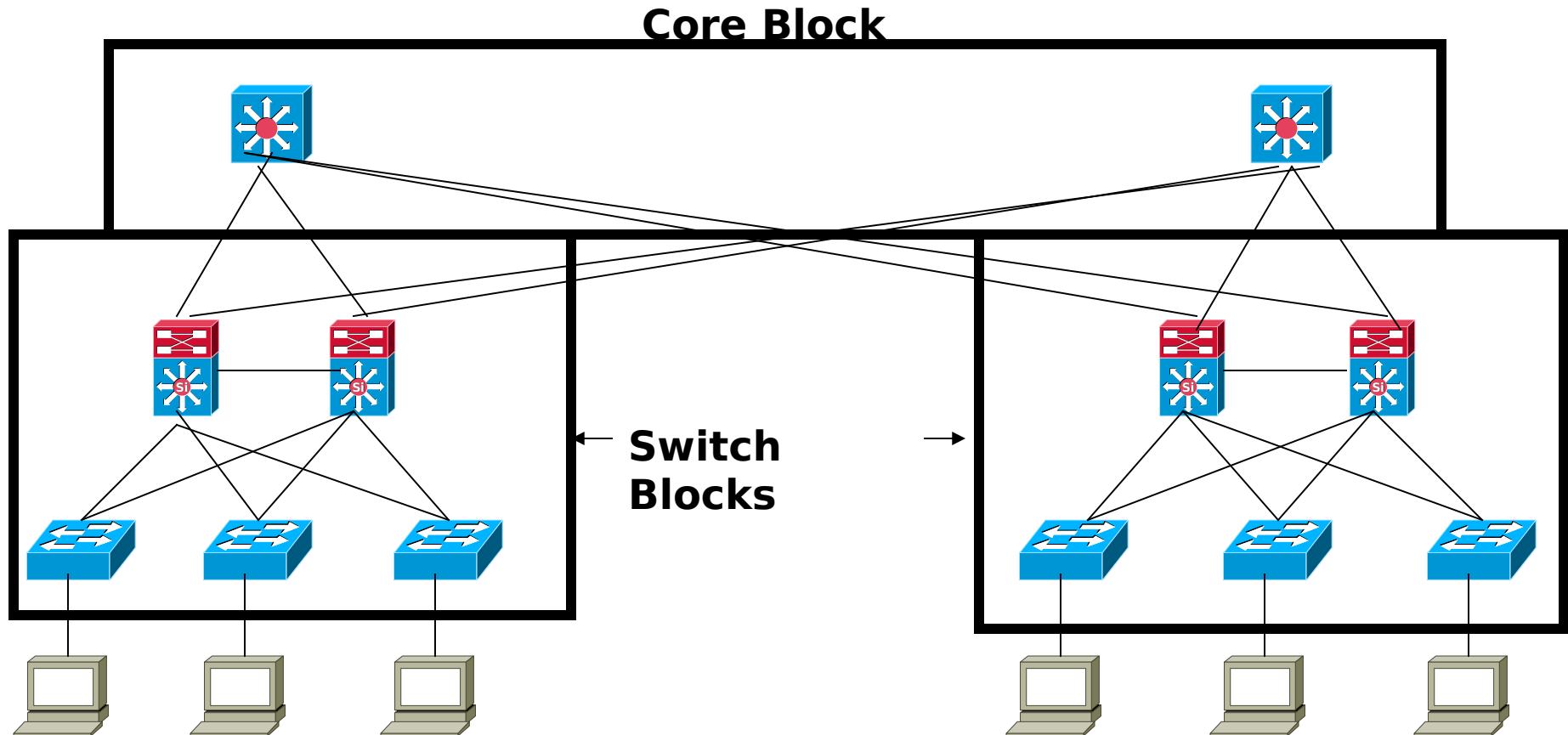
Core Layer



- **Fast transport to enterprise services**
- **No packet manipulation**

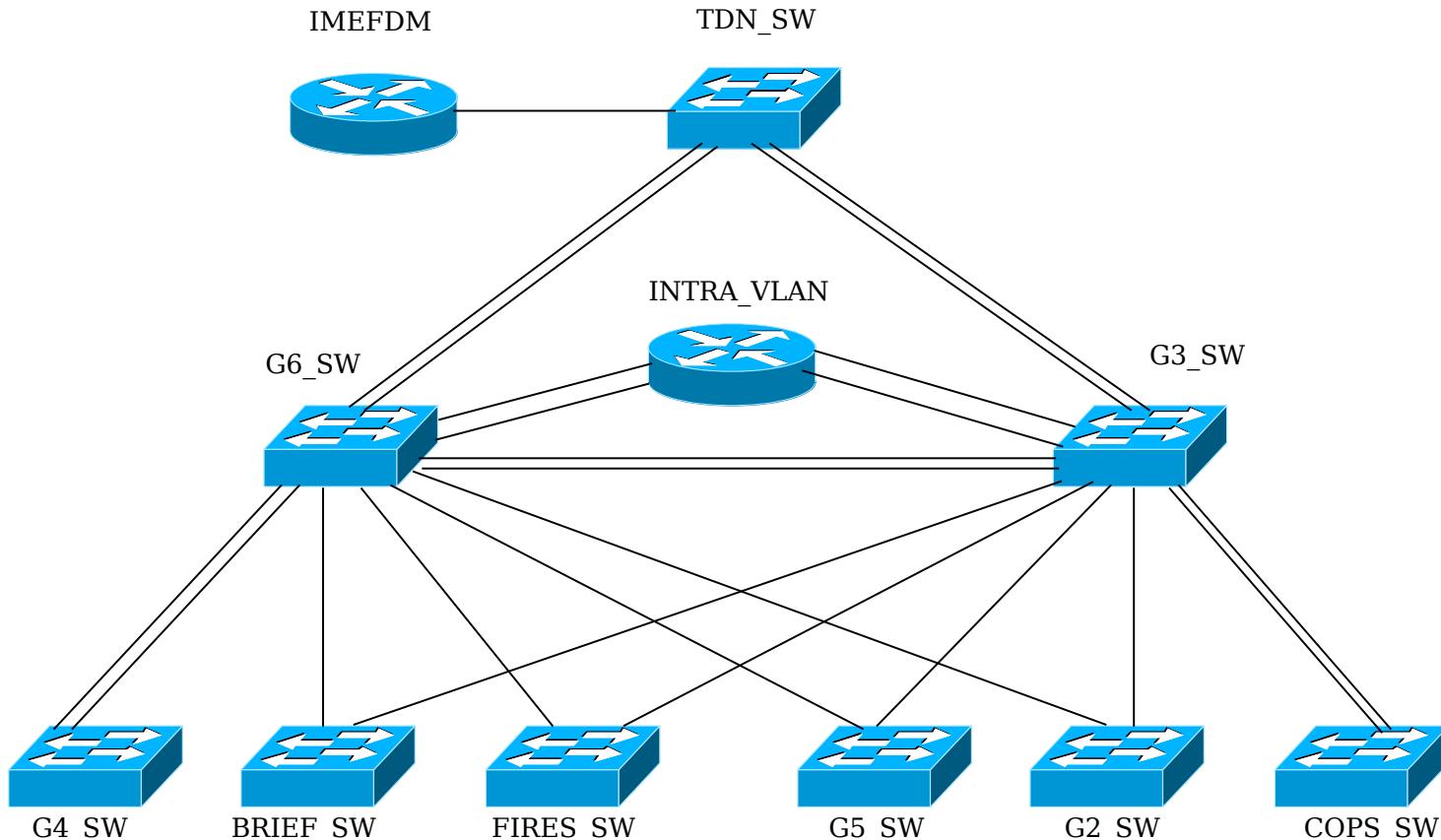
Building Block Method

MSTP

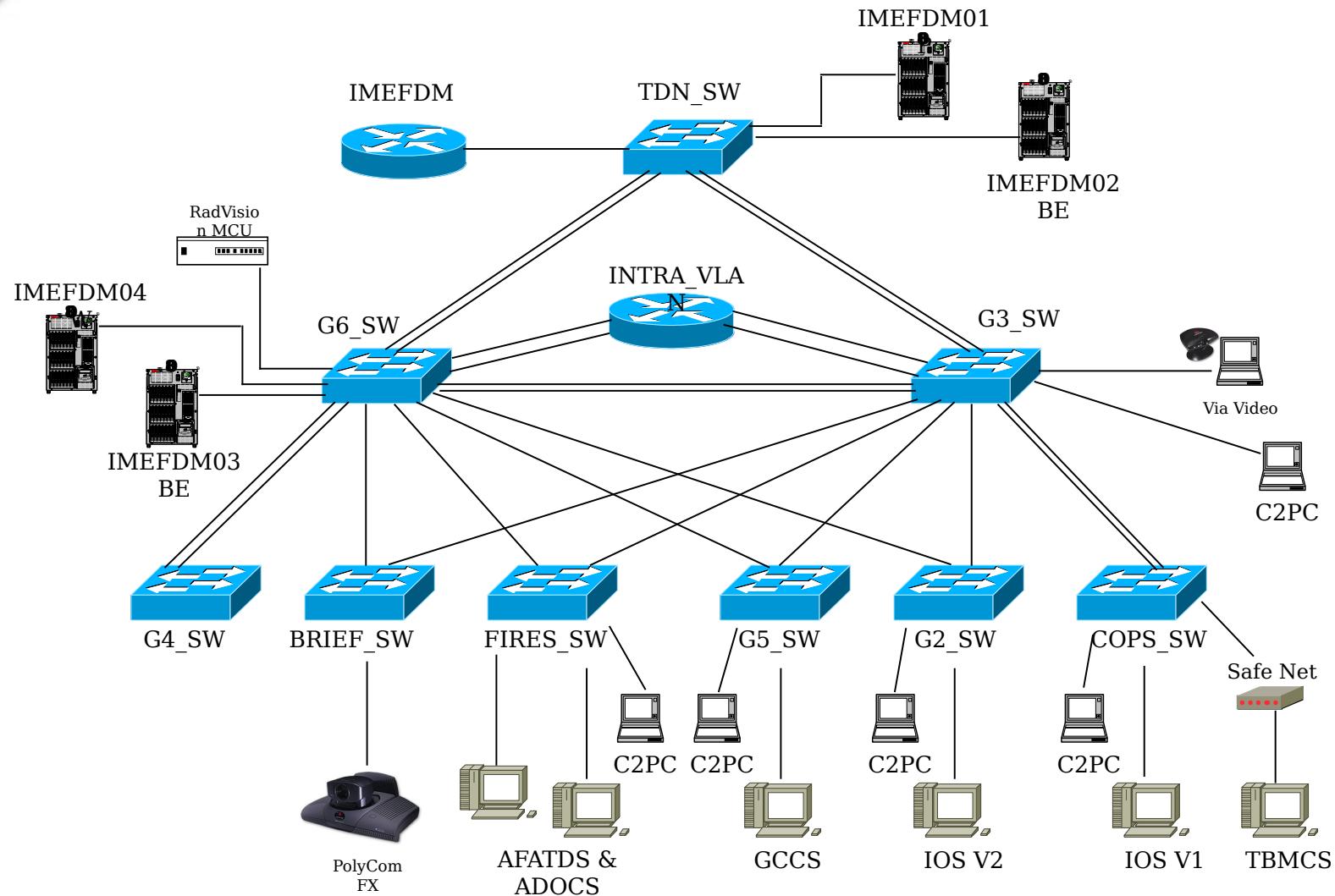


Switching Design (Round #2)

MSTP



Switching Design (C2 Systems)





Initial Start up

MSTP

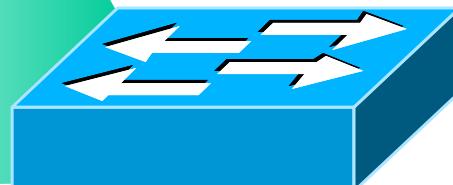
- System startup routines initiate switch software
- Initial startup uses default configuration parameters

~~Before you start the switch,
verify the cabling and console~~

~~connection~~

**2. Attach the power cable plug
to
the switch power supply
socket**

3. Observe the boot sequence
~~- LEDs on the switch chassis~~
~~- Cisco IOS software output
text~~

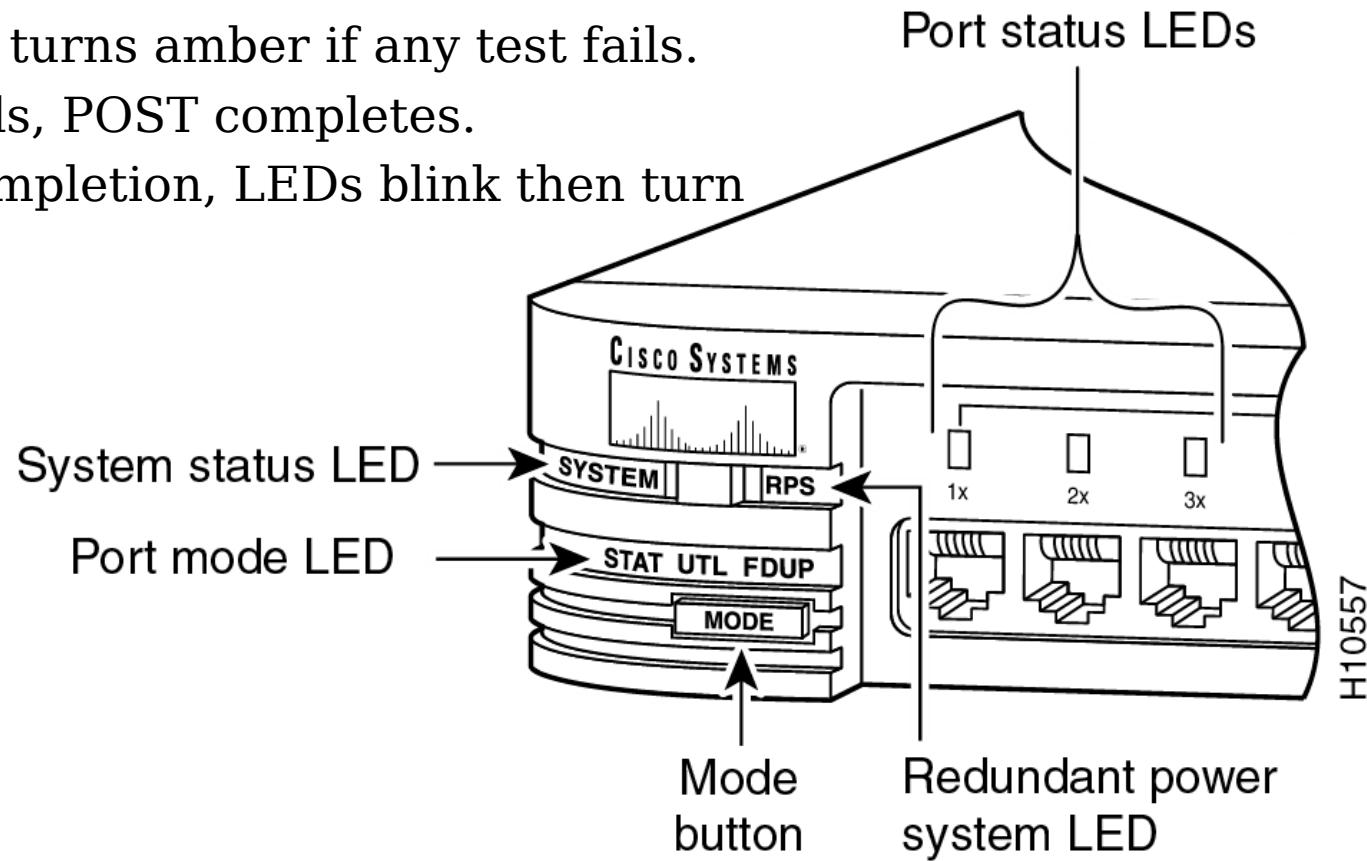




Switch LED Indicators

MSTP

1. At the start, all port LEDs are green.
2. Each LED turns off after its test completes.
3. If a test fails, its LED turns amber.
4. System LED turns amber if any test fails.
5. If no test fails, POST completes.
6. On POST completion, LEDs blink then turn off.



Command/Switch Based CLI

MSTP

- Command Based Switch (29xx, 35xx, and 4xxx)
 - Switch> (User Mode)
 - Switch# (Privilege Mode)
 - Switch (Config)# (Global Configuration Mode)
 - Switch (Config-if)#(Subinterface Config Mode)
 - Switch (Vlan)# (Vlan Database Configuration)
- Set Based Switch (4xxx, 5xxx, and 55xx)
 - Switch> (User Mode)
 - Switch (Config)# (Privilege Mode)



Configuring the Switch

MSTP



User EXEC Commands - Router>

ping
show (limited)
enable
etc...

Privileged EXEC Commands - Router#

all User EXEC commands
debug commands
reload
configure
etc...

Global Configuration Commands - Router(config)#

hostname
enable secret
ip route

interface ethernet
serial
bri
etc...

Interface Commands - Router(config-if)#

ip address
ipx address
encapsulation
shutdown / no shutdown
etc...

router rip
ospf
igrp
etc...

Routing Engine Commands - Router(config-router)#

network
version
auto-summary
etc...

line vty
console
etc...

Line Commands - Router(config-line)#

password
login
modem commands
etc...



Configuration Process

MSTP

- Lock down the Switch
 - Line Con 0, Line VTY 0 4, and Enable Secret
- Configure the Identity
 - Host name, Services, and Banners
- Configure Interfaces/Switchports
 - Assign switchports to VLANs and configure Trunks
- Configure the VLAN Database
 - VTP Domain and VLANs
- Configure Advanced parameters

Configuration Process



MSTP

STEP 1



Lock Down the Switch

MSTP

- Lock Down the Switch
 - Switch(config)#line con 0
 - Switch (config-line)#login
 - Switch (config-line)#password *your-password*
 - Switch (config)#line vty 0 4
 - Switch (config-line)#login
 - Switch (config-line)#password *your-password*
 - Switch (config)#enable secret *your-password*



Password Recovery

MSTP

1. Hold down the mode button on the left side of the front panel while reconnecting power to the switch. You can release the mode button a second or two after the LED above port 1x is no longer illuminated.
2. Type **flash_init**
3. Type **load_helper**
4. Type **dir flash:**
5. Type **rename flash:config.text flash:config.old** to rename the configuration file.
6. Type **boot** to restart the system.
7. Enter **N** at the prompt to start Setup Program, **Continue with the configuration dialog? [yes/no]:N**
8. At the switch prompt type **en** to enter privileged Exec mode.
9. Type **rename flash:config.old flash:config.text** to rename configuration file to its original name.
10. Copy the startup configuration into memory: **Switch#copy flash:config.text system:running-config**
11. Change the password: **Switch#Configure Terminal, Switch(Config)#no enable secret ! - This step is necessary if the switch had a bad enable secret password**
12. Write the running-config to the configuration file. (WR)

Configuration Process



MSTP

STEP 2



Configure the Identity

MSTP

- Switch (config)#hostname IMEF
- IMEF (config)#service timestamps debug local
- IMEF (config)#service timestamps log local
- IMEF (config)#service password-encryption
- IMEF (config)#clock timezone EST 5
- IMEF#clock set 16:27:00 May 22 2002
- IMEF (config)#banner motd #
- IMEF (config)#banner login #

Configuration Process



MSTP

STEP 3



Configure Interfaces/Switchports

MSTP

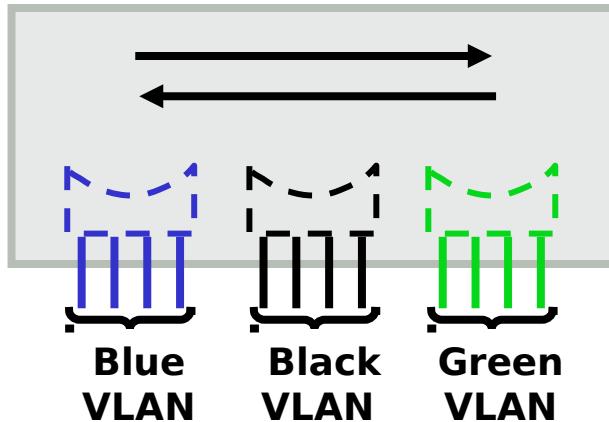
- IMEF(config)#interface fa 0/1
- IMEF(config-)#switchport access vlan 25
- IMEF(config-)#port group 3
- IMEF(config-)#switchport mode trunk
- IMEF(config-)#switchport trunk encapsulation dot1q
- IMEF(config-)#switchport trunk encapsulation isl
- IMEF(config-)#switch trunk native vlan 88

VLAN Operations

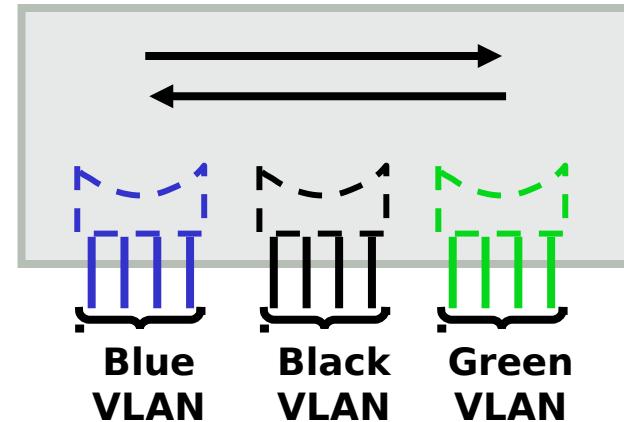


MSTP

Switch A



Switch B

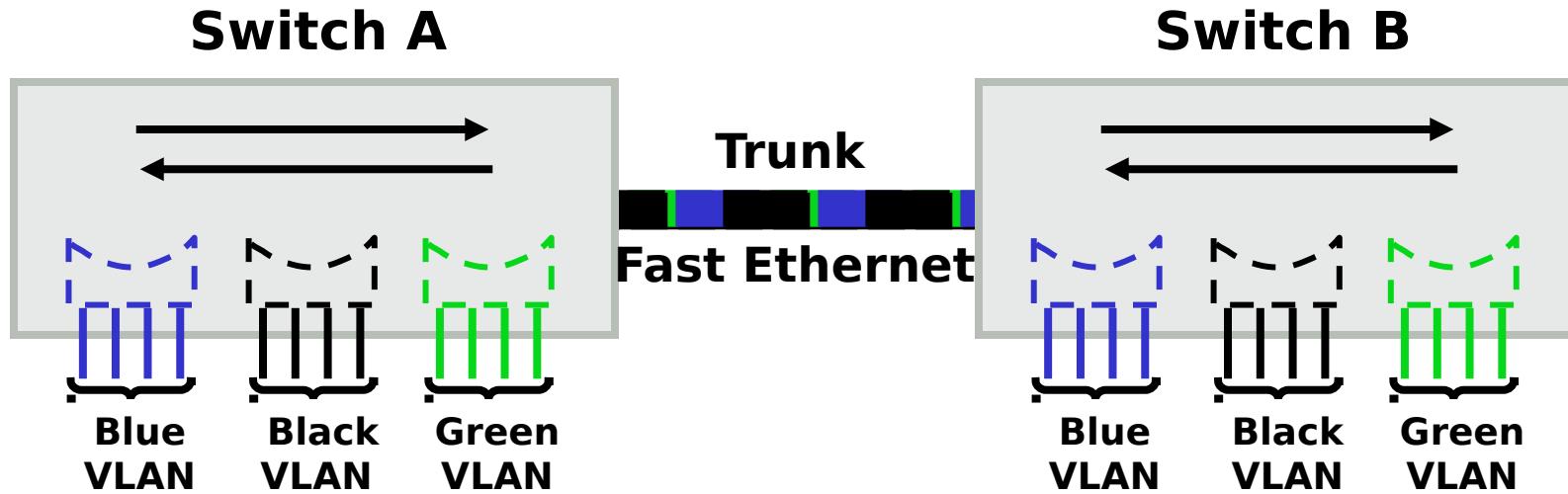


- Each logical VLAN is like a separate physical bridge
- VLANs can span across multiple switches

VLAN Operations



MSTP



- **Each logical VLAN is like a separate physical bridge**
- **VLANs can span across multiple switches**
- **A trunks carries traffic for multiple VLANs**

Configuration Process



MSTP

STEP 4



Configure VLAN Database

MSTP

- Switch# Vlan database
- Switch (Vlan)#vtp server (client/transparent)
- Switch (Vlan)#vtp domain *IMEF*
- Switch (Vlan)#vlan 25 name 205.54.25.0/24
- Switch (Vlan)#exit
- Switch (Vlan)#apply
- Switch (Vlan)#abort
- Switch (Vlan)#reset



MSTP

WHY VLANS?



Switch Functions

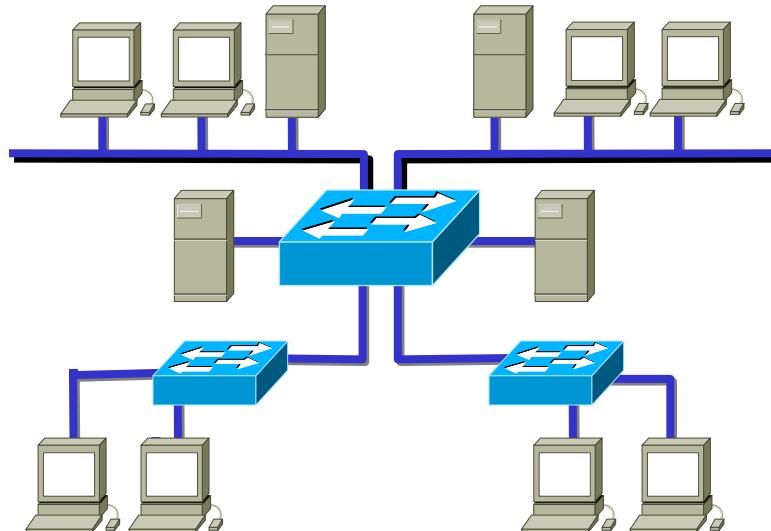
MSTP

- Break Up Collision Domains
 - Layer 2 Switching is Hardware Based
 - Application-Specific Integrated Circuits (ASICs)
 - No modification to Layer 2 Header
- Provide Segmentation
 - Each Port is a segment
 - Can achieve Gigabit Speeds



Three Main Tasks

MSTP

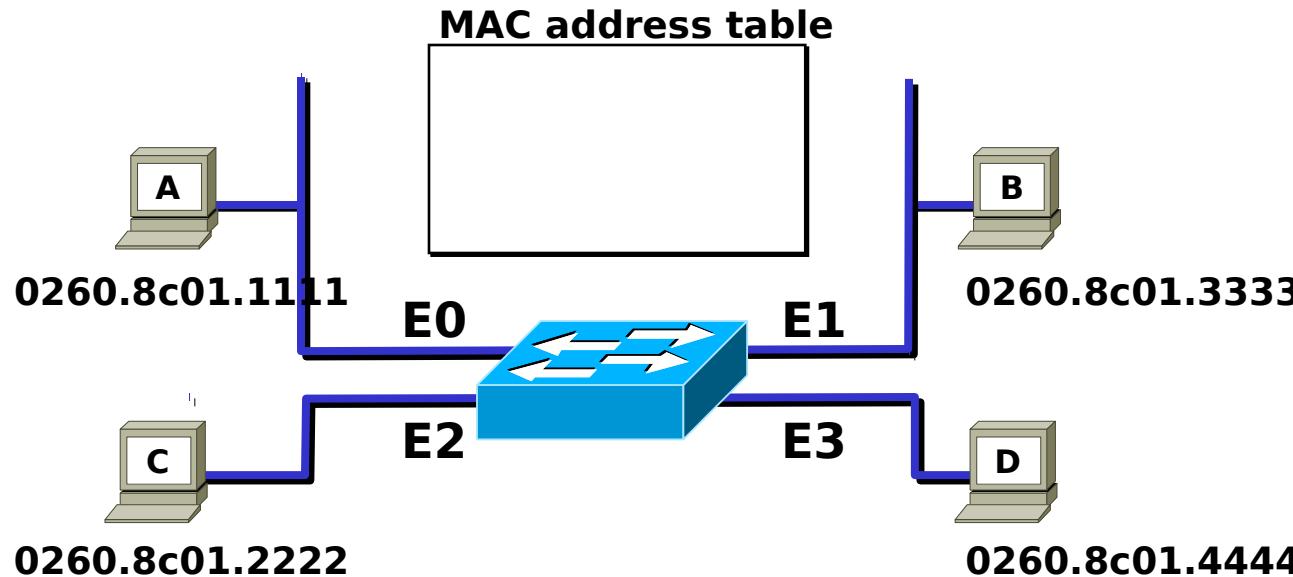


- Address learning
- Forward/filter decision
- Loop avoidance



Learning Host Locations

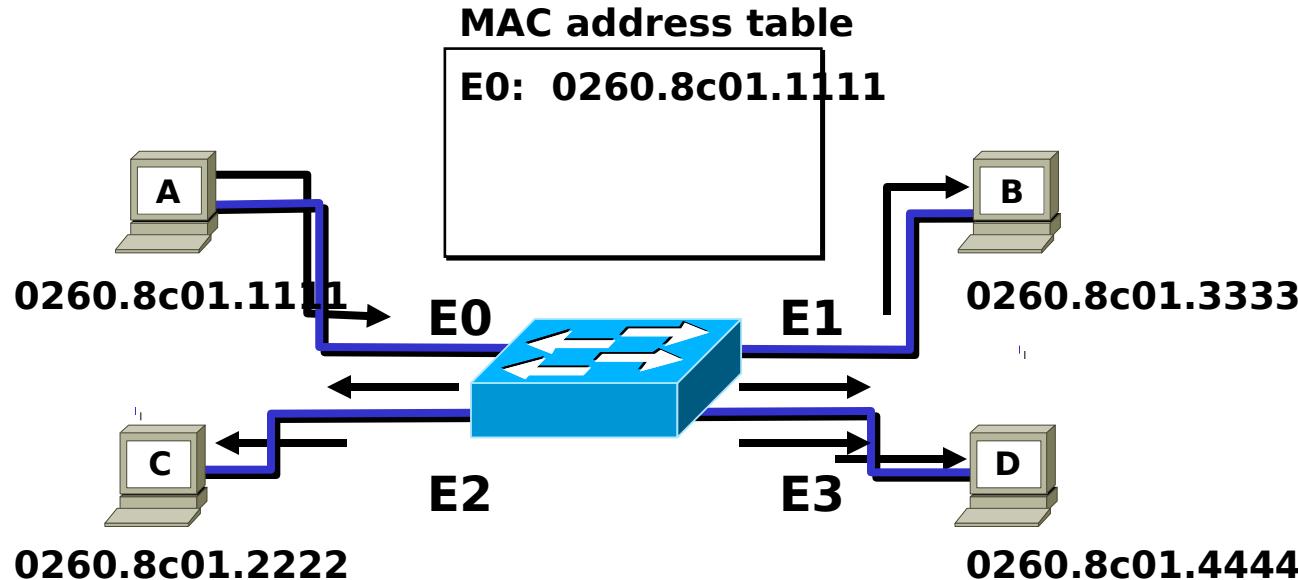
MSTP



- Initial MAC address table is empty

Learning Host Locations

MSTP

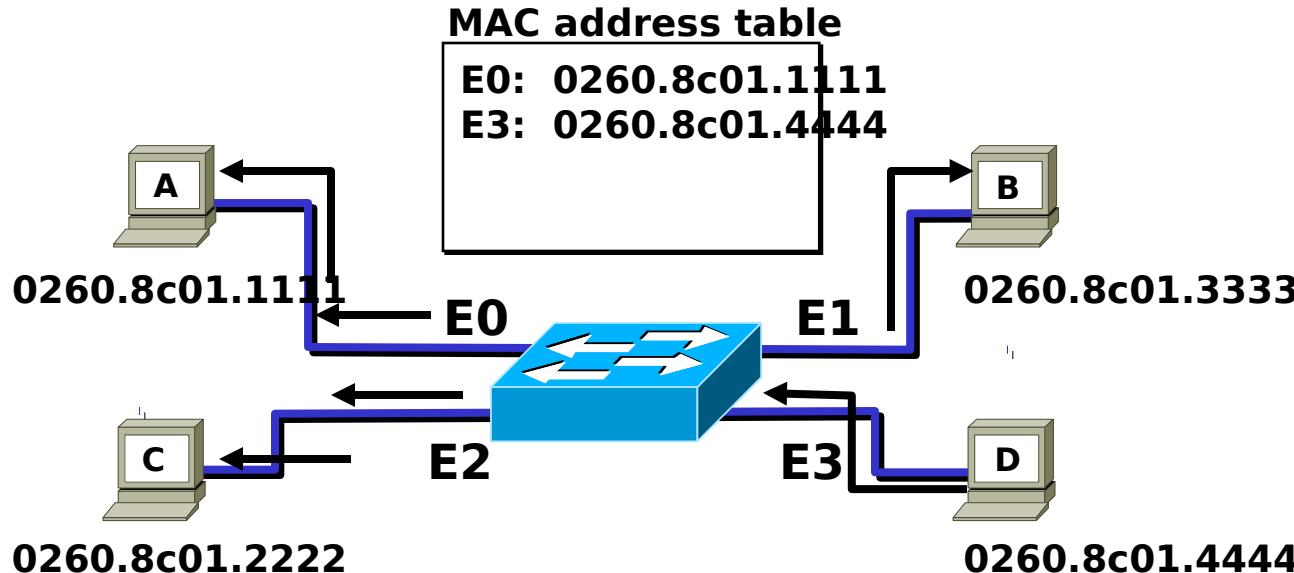


- **Station A sends a frame to Station C**
- **Switch caches station A MAC address to port E0 by learning the source address of data frames**
- **The frame from station A to station C is flooded out to all ports except port E0 (unknown unicasts are flooded)**

Learning Host Locations



MSTP

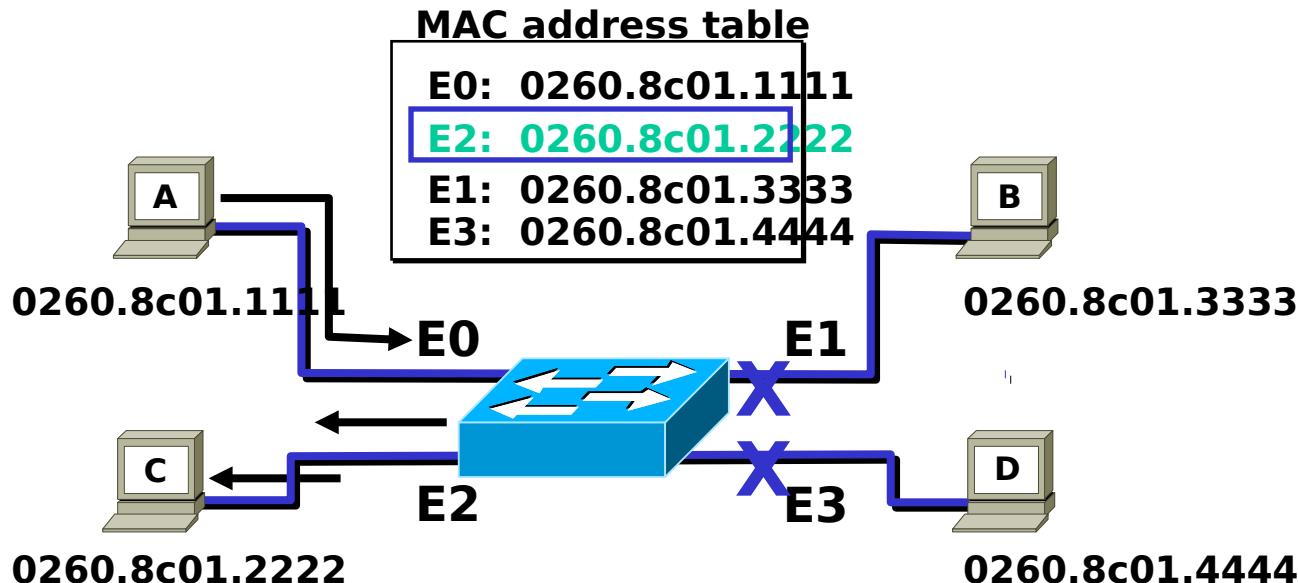


- Station D sends a frame to station C
- Switch caches station D MAC address to port E3 by learning the source Address of data frames
- The frame from station D to station C is flooded out to all ports except port E3 (unknown unicasts are



Filtering Frames

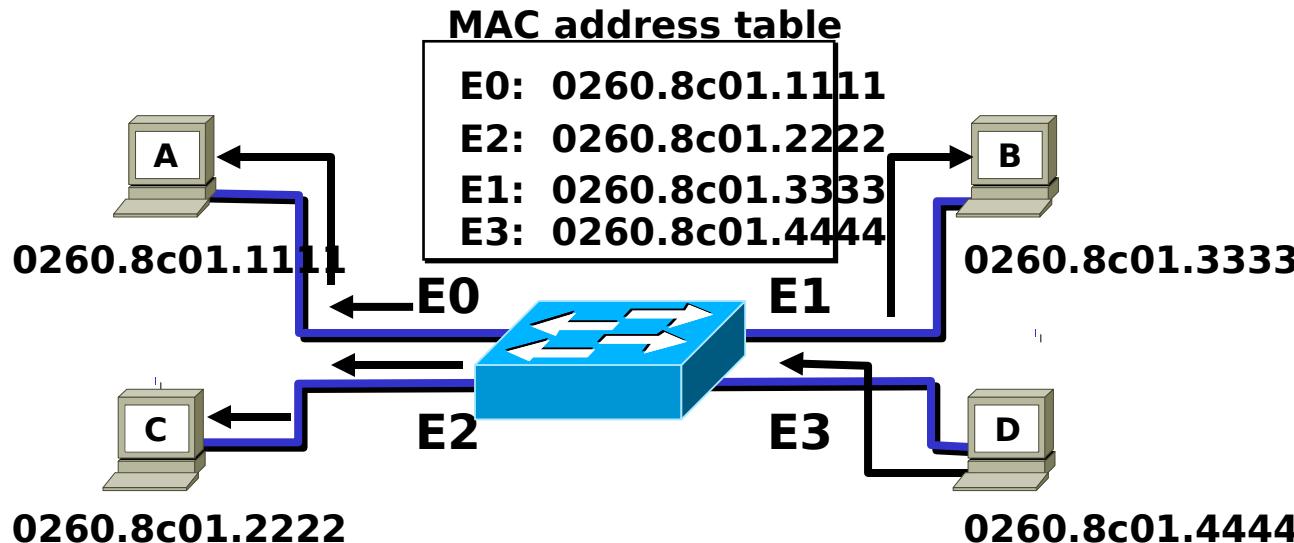
MSTP



- Station A sends a frame to station C
- Destination is known, frame is not flooded

Broadcast and Multicast Frames

MSTP



- Station D sends a broadcast or multicast frame
- Broadcast and multicast frames are flooded to all ports other than the



LAN Switching Methods

MSTP

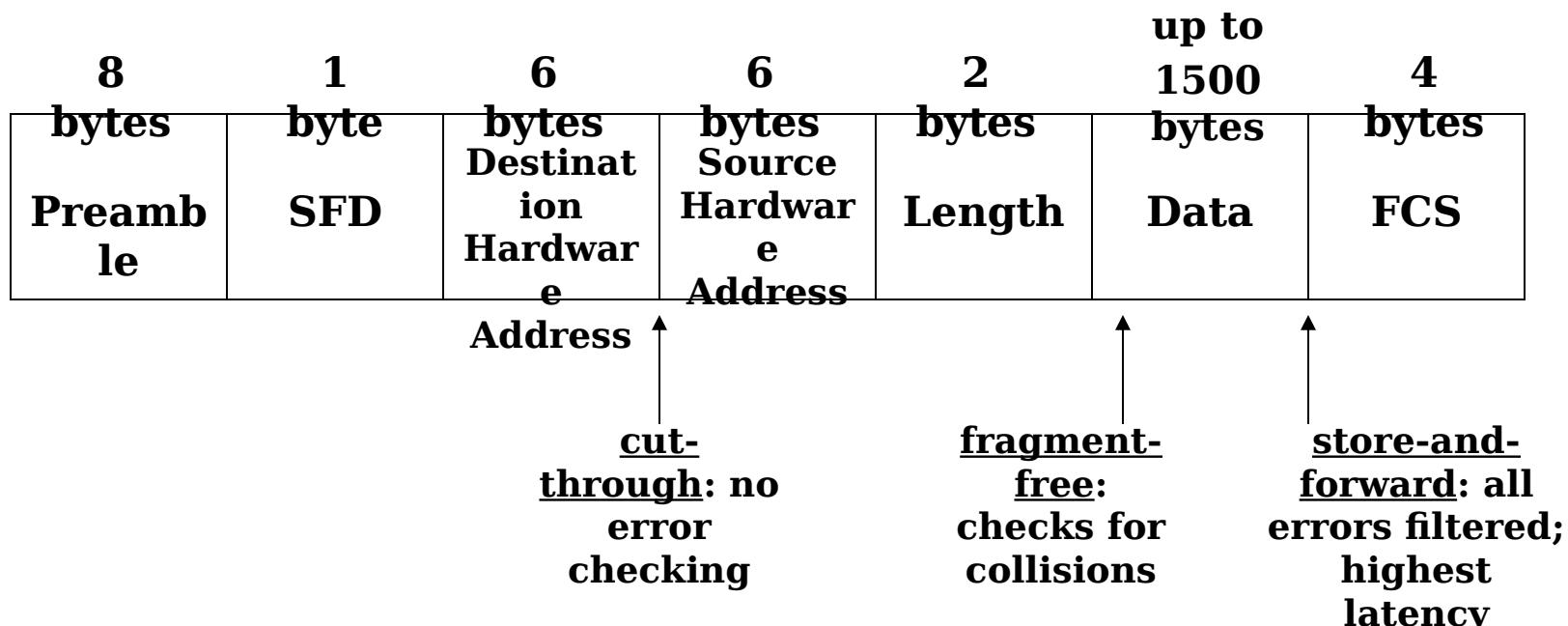
- There are three different methods in which these frames can be forwarded or filtered.
 - **Store-and-Forward**
 - **Cut-through**
 - **Fragment-free**



Switching Types

MSTP

- Here in this picture we will try to show where the different points are that the 3 switching modes actually take place in the frame.

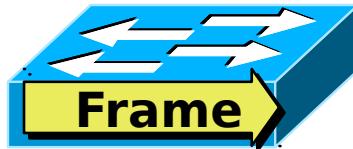




Frames Through a Switch

MSTP

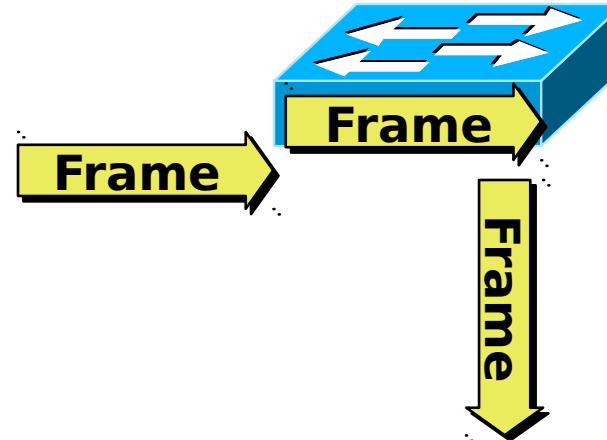
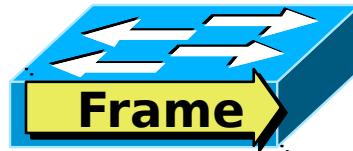
- Cut-through
 - Switch checks destination address and immediately begins forwarding frame





Frames through a Switch

- Cut-through
 - Switch checks destination address and immediately begins forwarding frame
- Store and forward
 - Complete frame is received and checked before forwarding

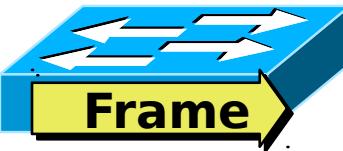
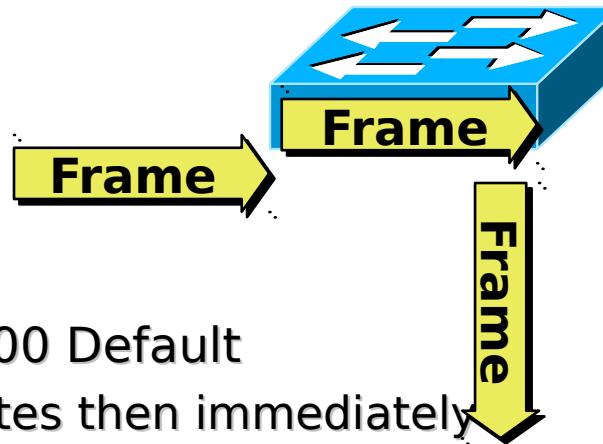
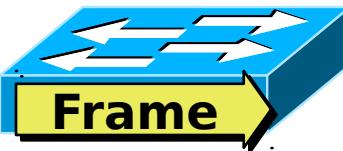


Frames through a Switch



MSTP

- Cut-through
 - Switch checks destination address and immediately begins forwarding frame
- Store and forward
 - Complete frame is received and checked before forwarding
- Fragment free (modified cut-through)—Cat1900 Default
 - Switch checks the first 64 bytes then immediately begins forwarding frame

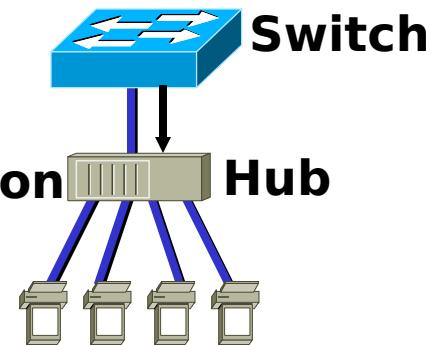


Duplex Overview

MSTP

Half duplex (CSMA/CD)

- Unidirectional data flow
- Higher potential for collision
- Hubs connectivity



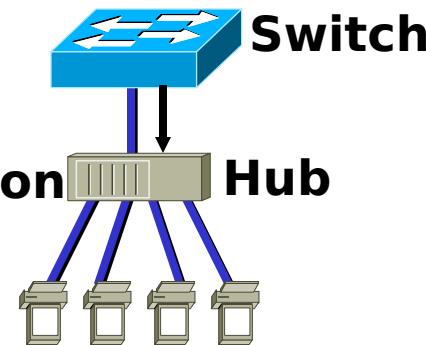
Duplex Overview



MSTP

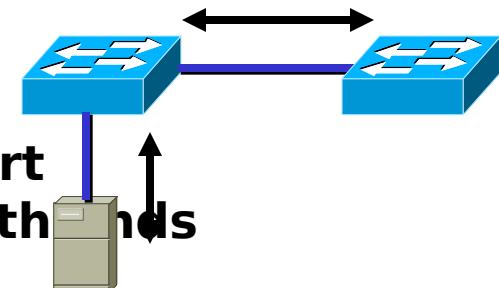
Half duplex (CSMA/CD)

- Unidirectional data flow
- Higher potential for collision
- Hubs connectivity



Full duplex

- Point-to-point only
- Attached to dedicated switched port
- Requires full-duplex support on both ends
- Collision free
- Collision detect circuit disabled





Common Work Groups

MSTP

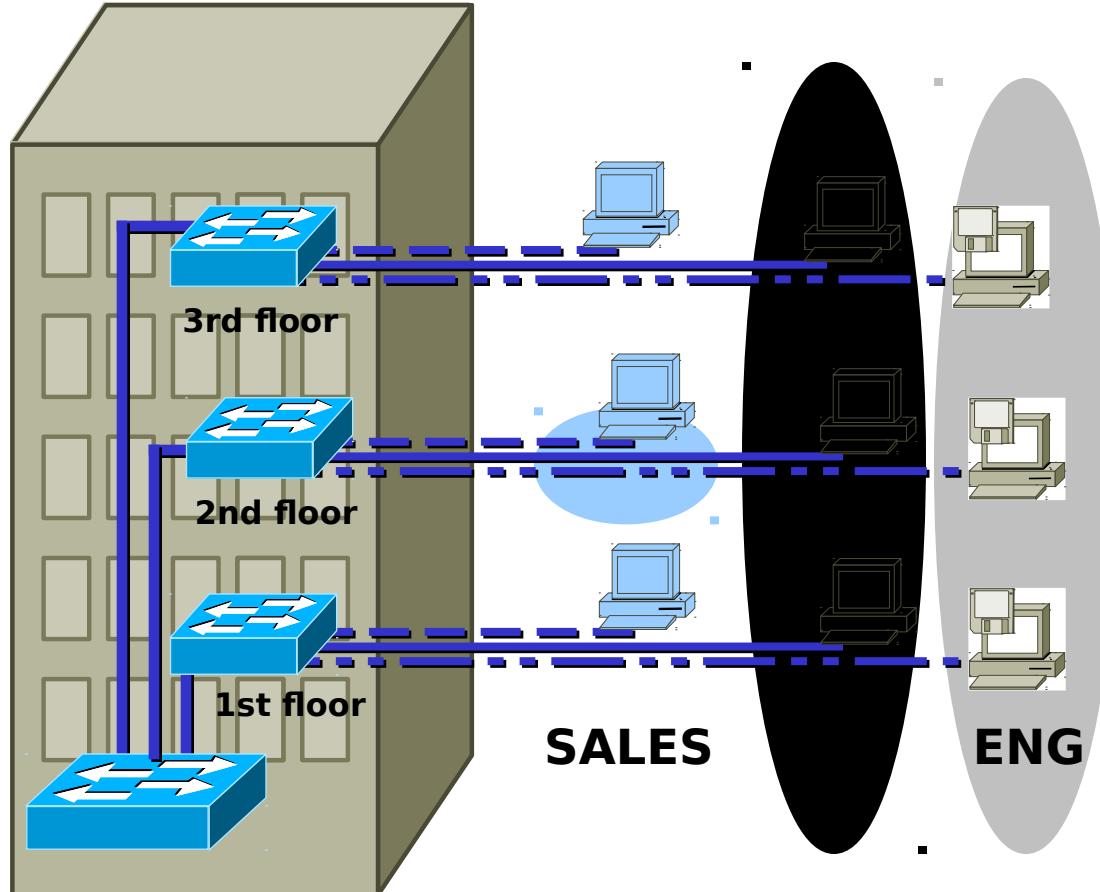
Upon completion of this chapter, you will be able to perform the following tasks:

- Configure a VLAN
- Configure VLAN Trunking Protocol (VTP)
- Configure a switch for trunking
- Verify VLAN connectivity
- Verify spanning-tree operations

VLAN Overview



MSTP



- Segmentation
- Flexibility
- Security

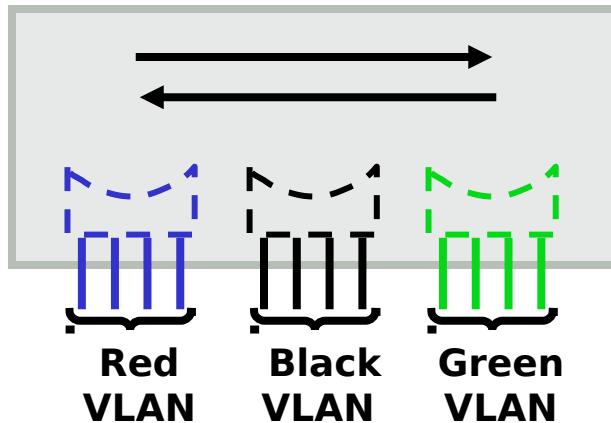
VLAN = A broadcast domain = Logical network (subnet)



VLAN Operations

MSTP

Switch A



- **Each logical VLAN is like a separate physical bridge**



VLAN Guidelines

MSTP

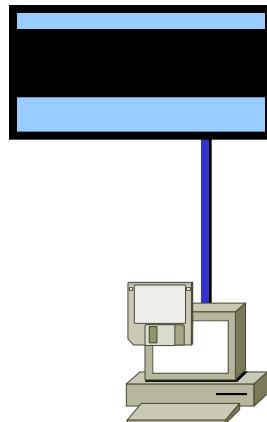
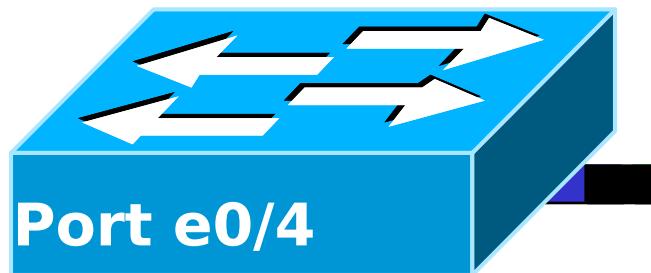
- Maximum number of VLANs, switch-dependent
 - Catalyst 6XXX, 55XX, 35XX, support 1005 VLANs
 - Catalyst 1900 supports 64 VLANs
- 5 Factory Default VLANs
 - VLAN 1 (Can not change VLAN 1 name)
 - VLAN 1001-1005
- CDP and VTP advertisements are sent on VLAN1
 - Must be in VTP server or transparent mode to create, add, or delete VLANs

VLAN Membership Modes

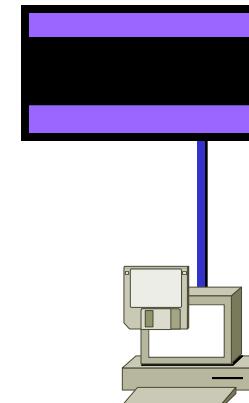
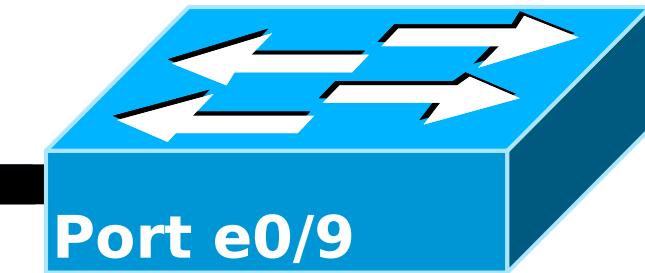


MSTP

Static VLAN



Dynamic VLAN



MAC = 1111.1111.1111

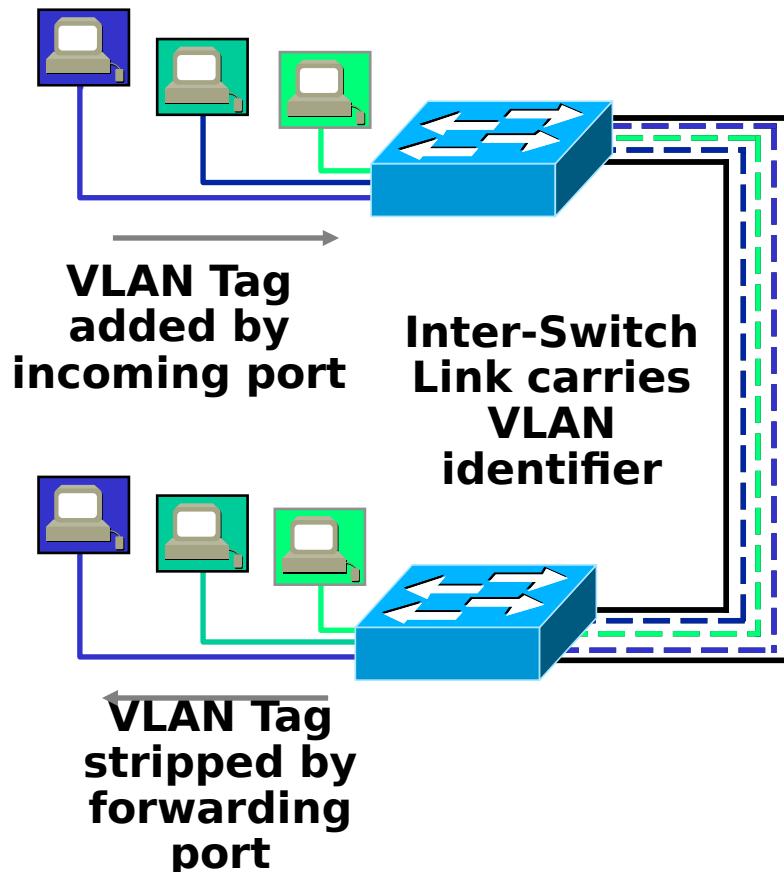
1111.1111.1111 = vlan 10



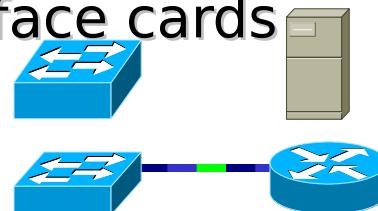
ISL Tagging

MSTP

ISL trunks enable VLANs across a backbone

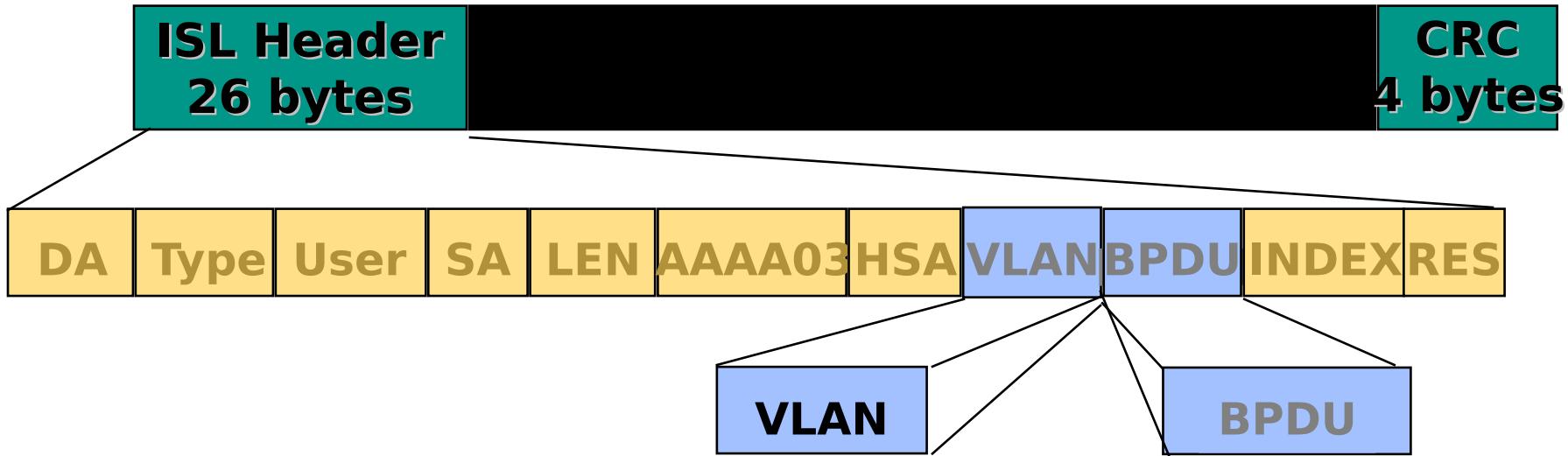


- performed with ASIC (Application Specific Integrated Circuit)
- Not intrusive to client stations, client does not see the ISL header
 - Effective between switches, routers and switches, switches and servers with ISL network interface cards



ISL Encapsulation

MSTP



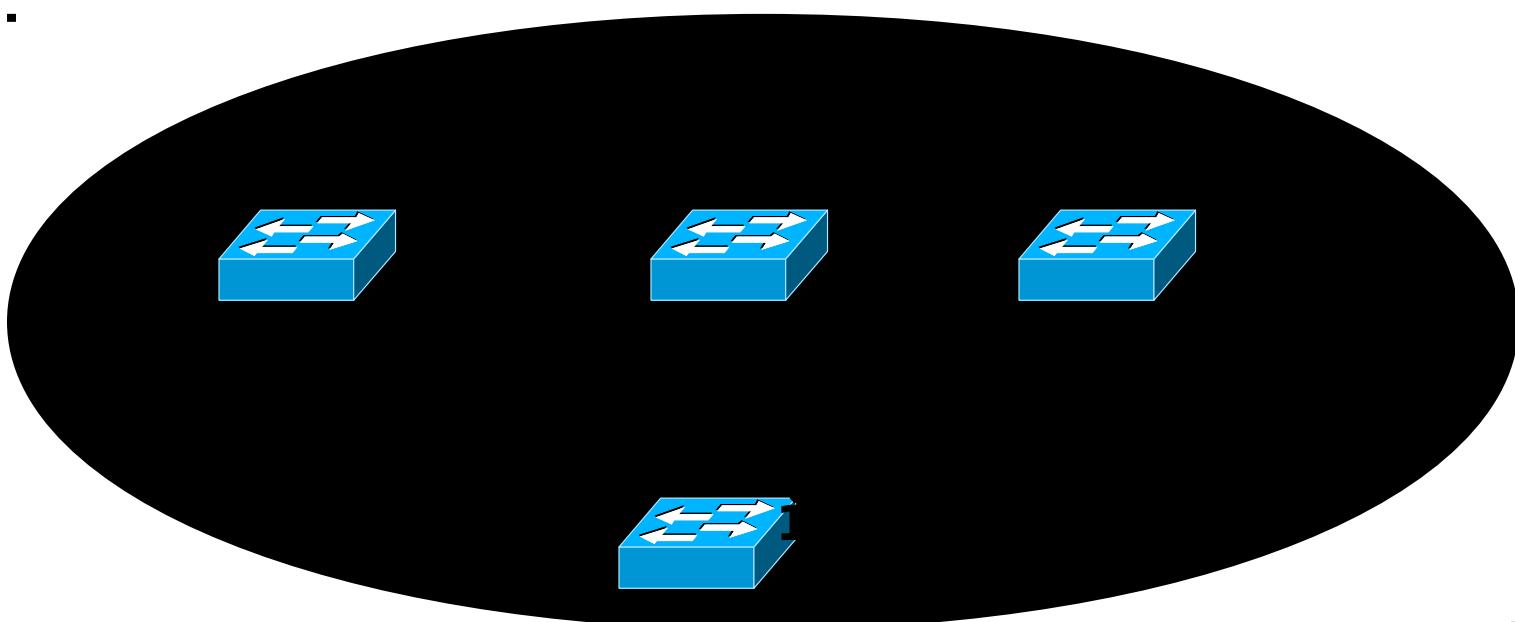
- Frames encapsulated with ISL header and CRC
- Support for many VLANs (1024)
- VLAN field
- BPDU bit

VLAN Trunking Protocol (VTP)



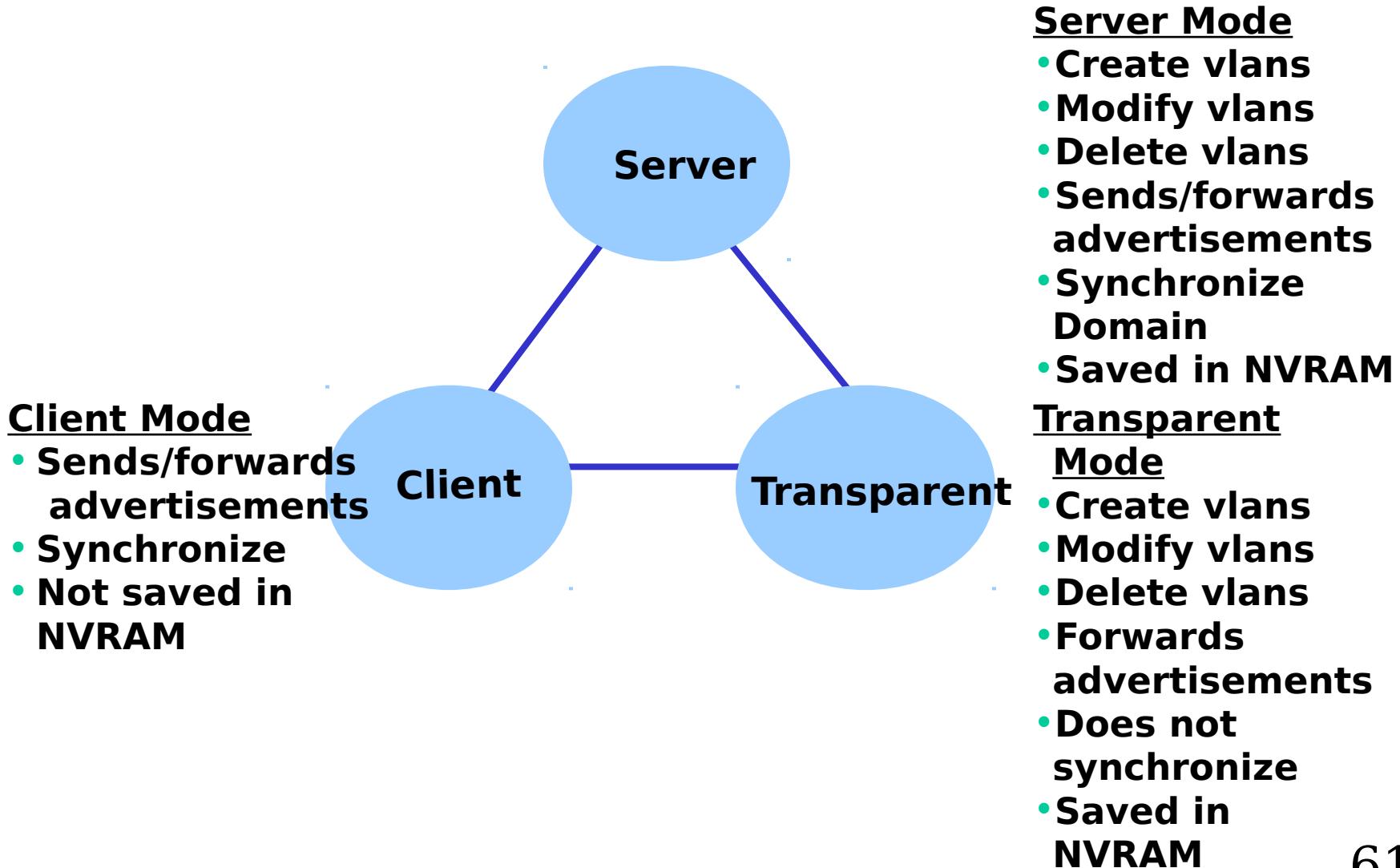
MSTP

- A messaging system that advertises VLAN configuration information
- Maintains VLAN configuration consistency throughout a common administrative domain
- VTP sends advertisements on trunk ports only
- Support mixed media trunks (Fast Ethernet, FDDI, ATM)



VTP Modes

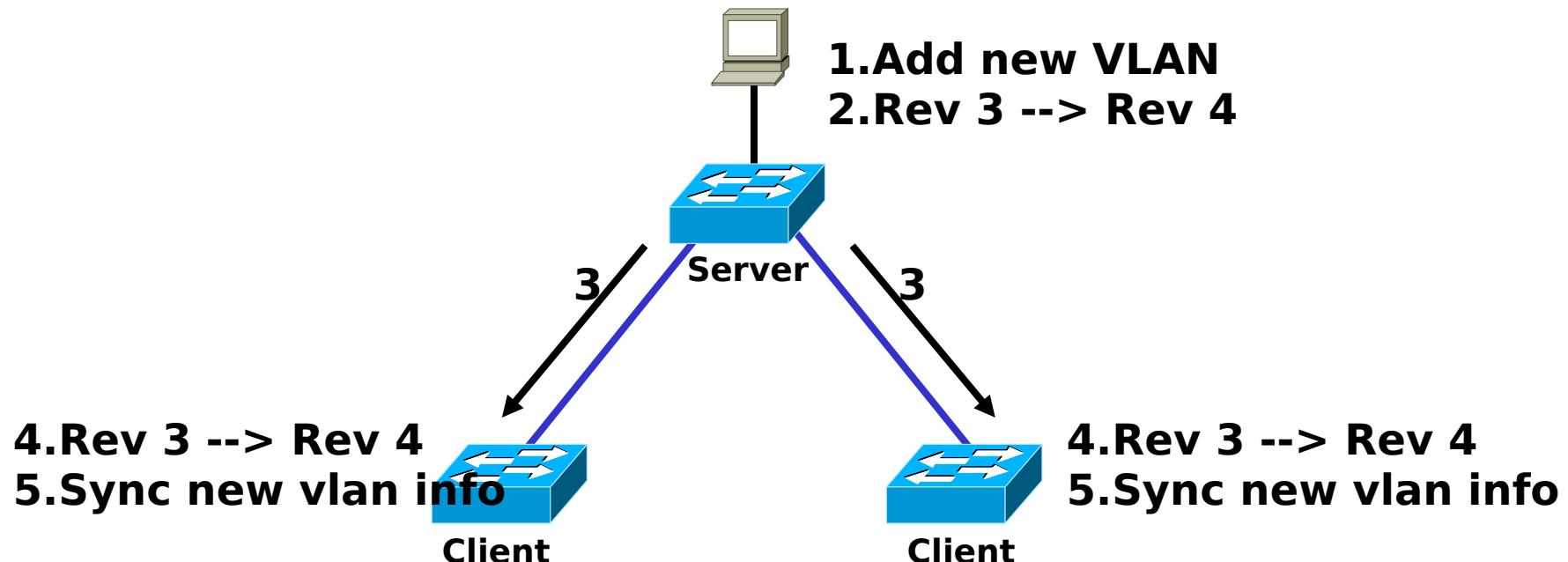
MSTP



How VTP Works

MSTP

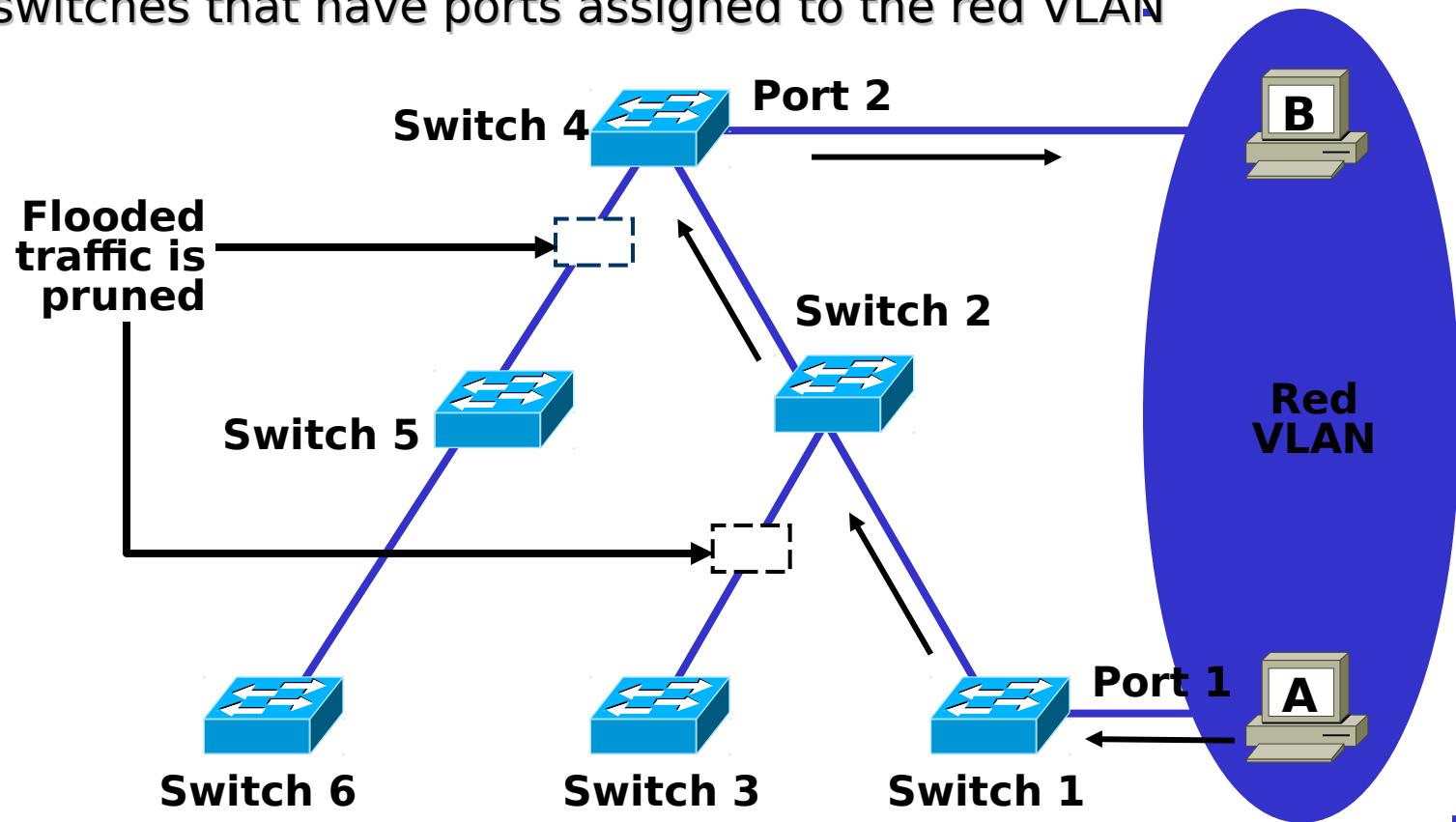
- VTP advertisements are sent as multicast frames
- VTP servers and clients synchronized to latest revision number
- VTP advertisement are sent every five minutes or when there is a change



VTP Pruning

MSTP

- Increases available bandwidth by reducing unnecessary flooded traffic
- Example: Station A sends a broadcast, broadcast is only flooded to switches that have ports assigned to the red VLAN



Configuration Process



MSTP

STEP 5



Configure Advanced

MSTP

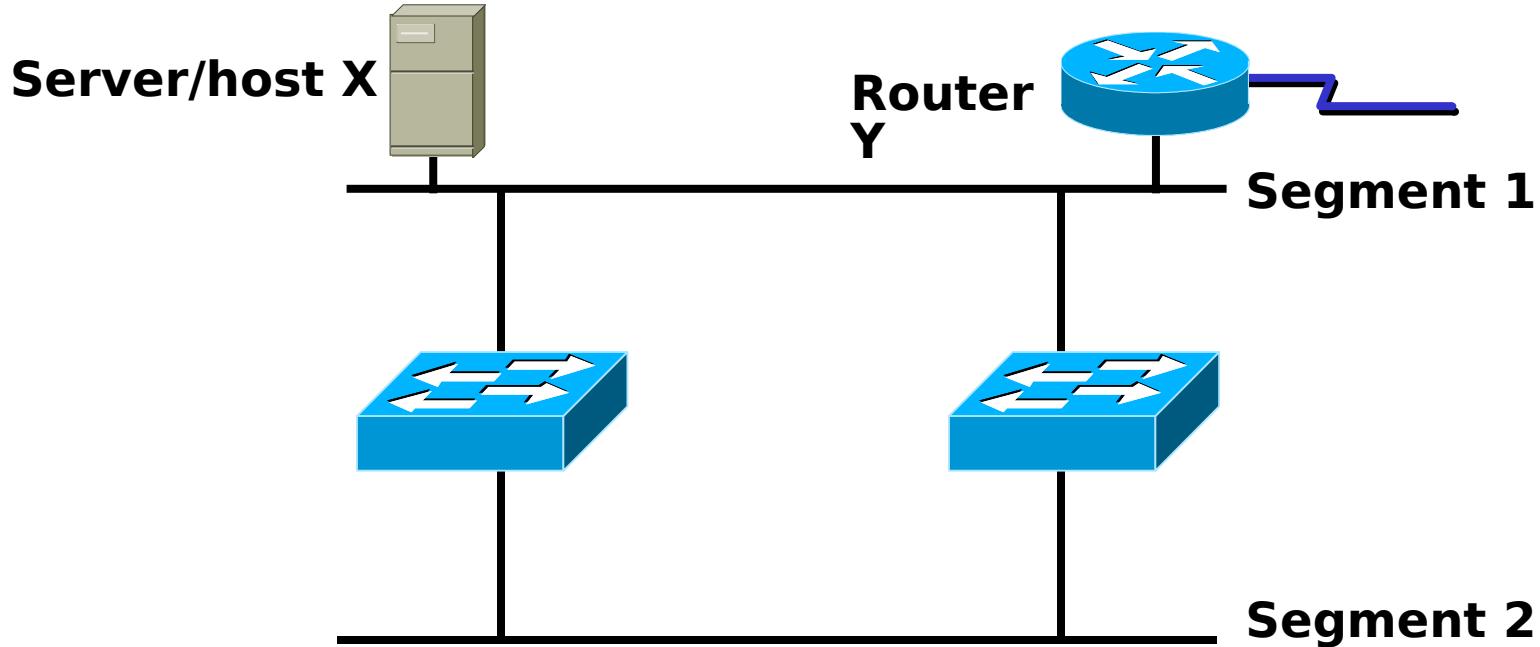
Parameter

- Spanning Tree S:
 - Root Switch/Bridge
 - Per VLAN Spanning Tree
 - Command based v/s Set Based CLI
- Quality of Service (QoS)
- Password Recovery



Redundant Topology

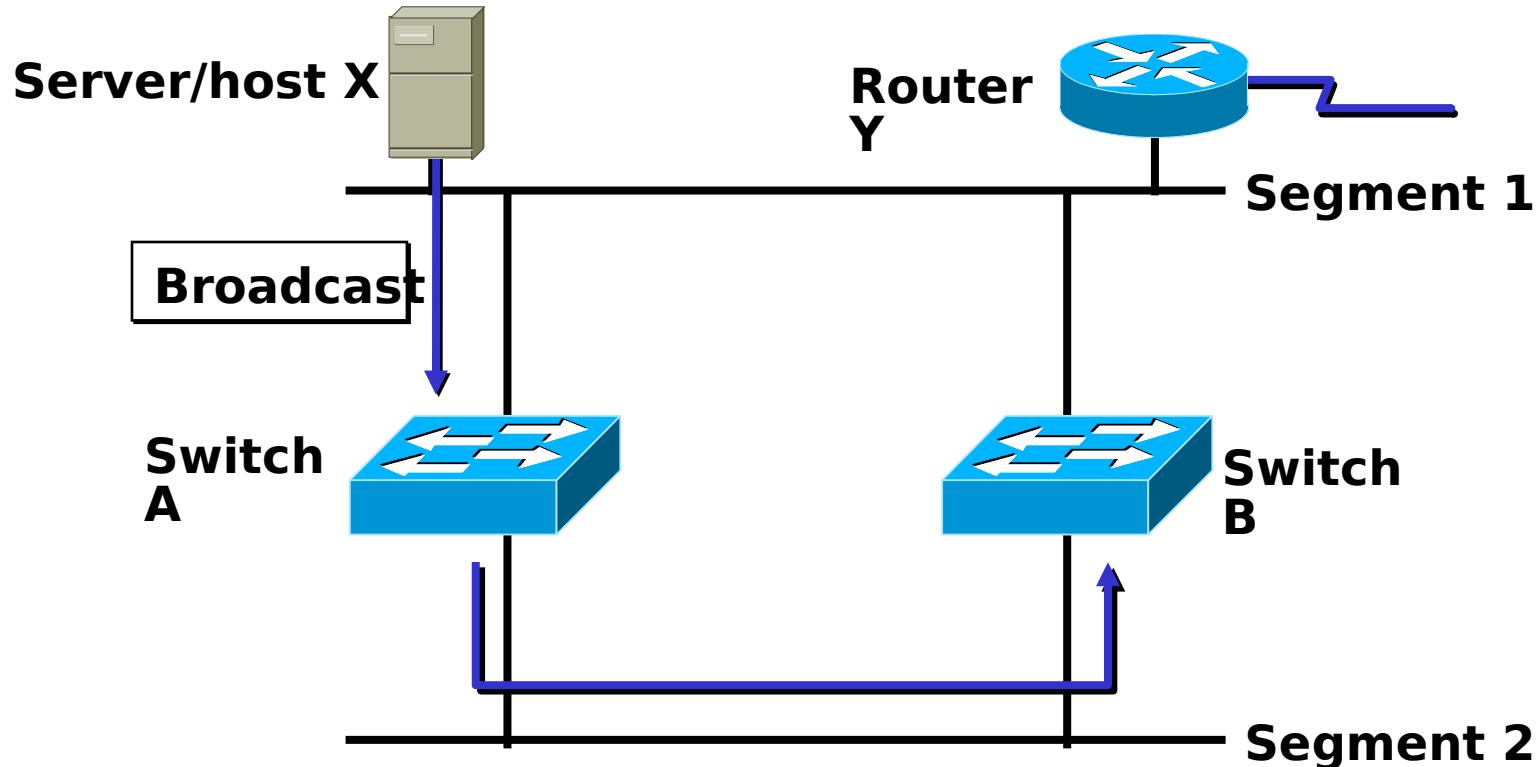
MSTP



- Redundant topology eliminates single points of failure
- Redundant topology causes broadcast storms, multiple frame copies, and MAC address table instability problems

Broadcast Storms

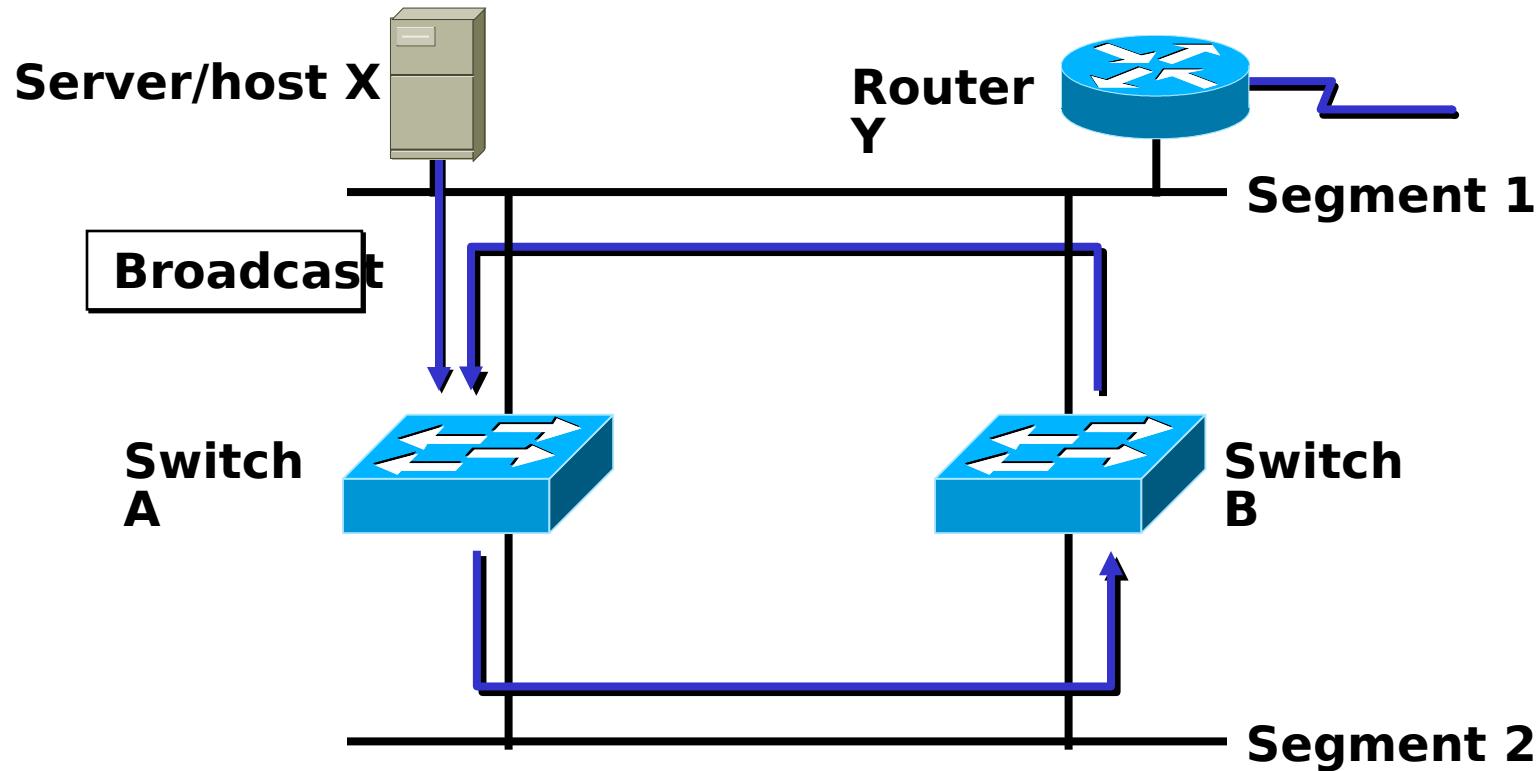
MSTP



Host X sends a Broadcast

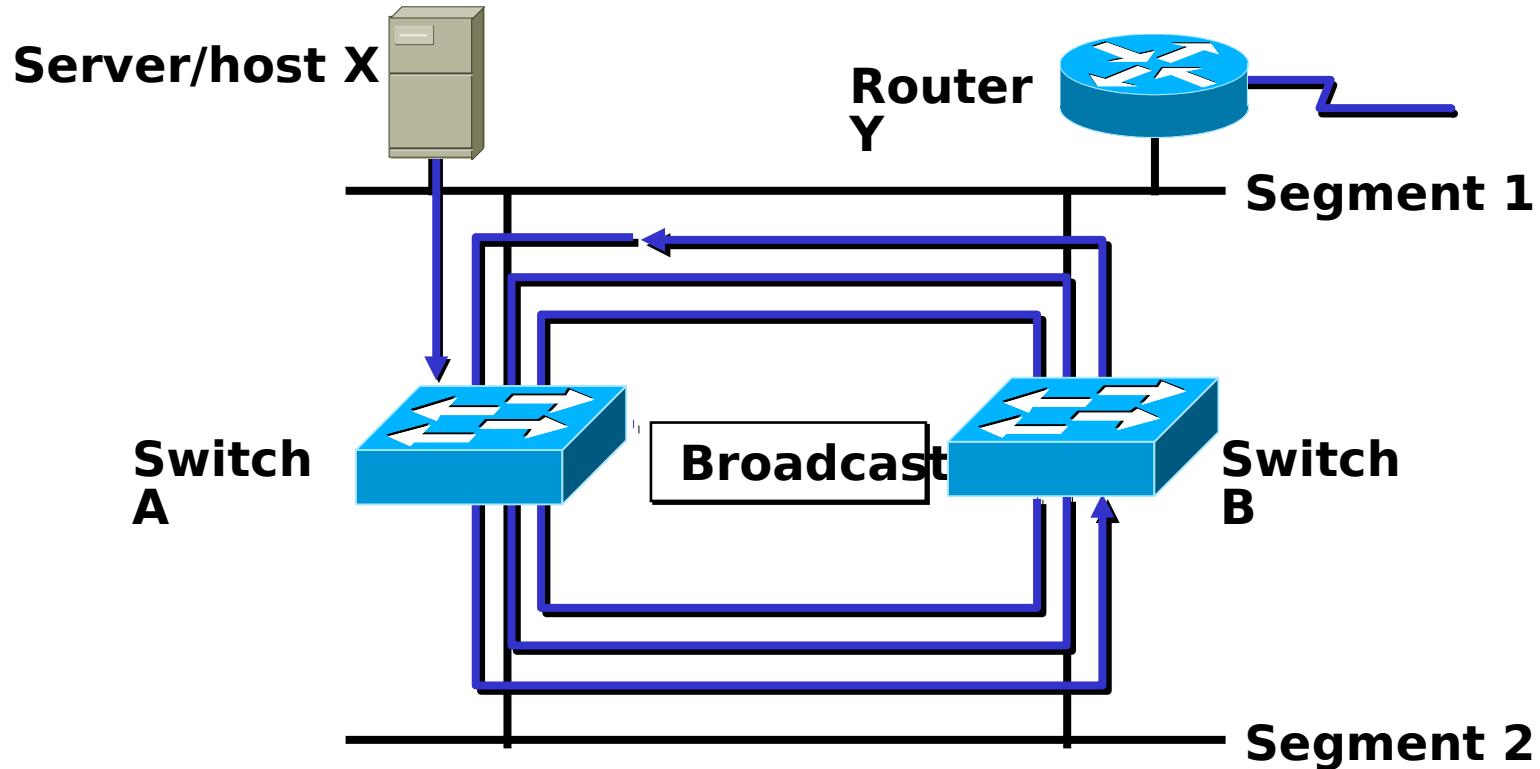
Broadcast Storms

MSTP



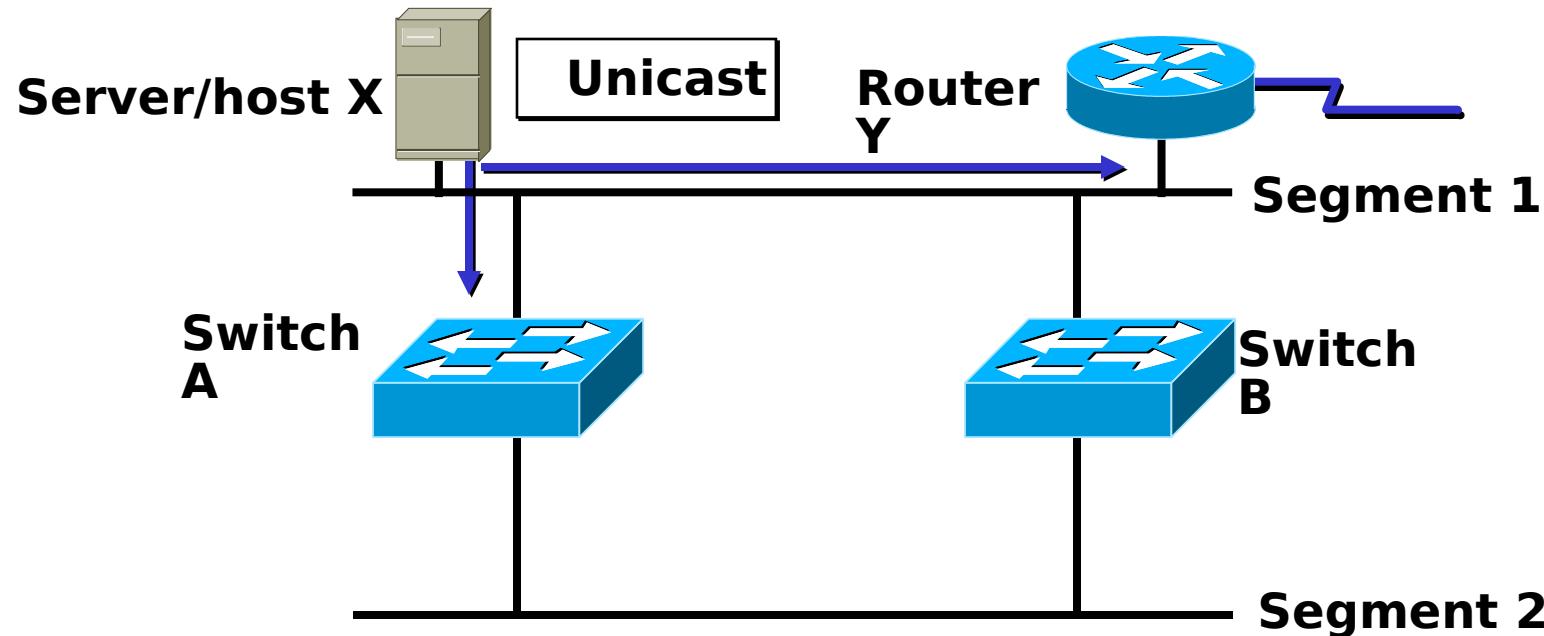
Host X sends a Broadcast

Broadcast Storms



Switches continue to propagate broadcast traffic over and over

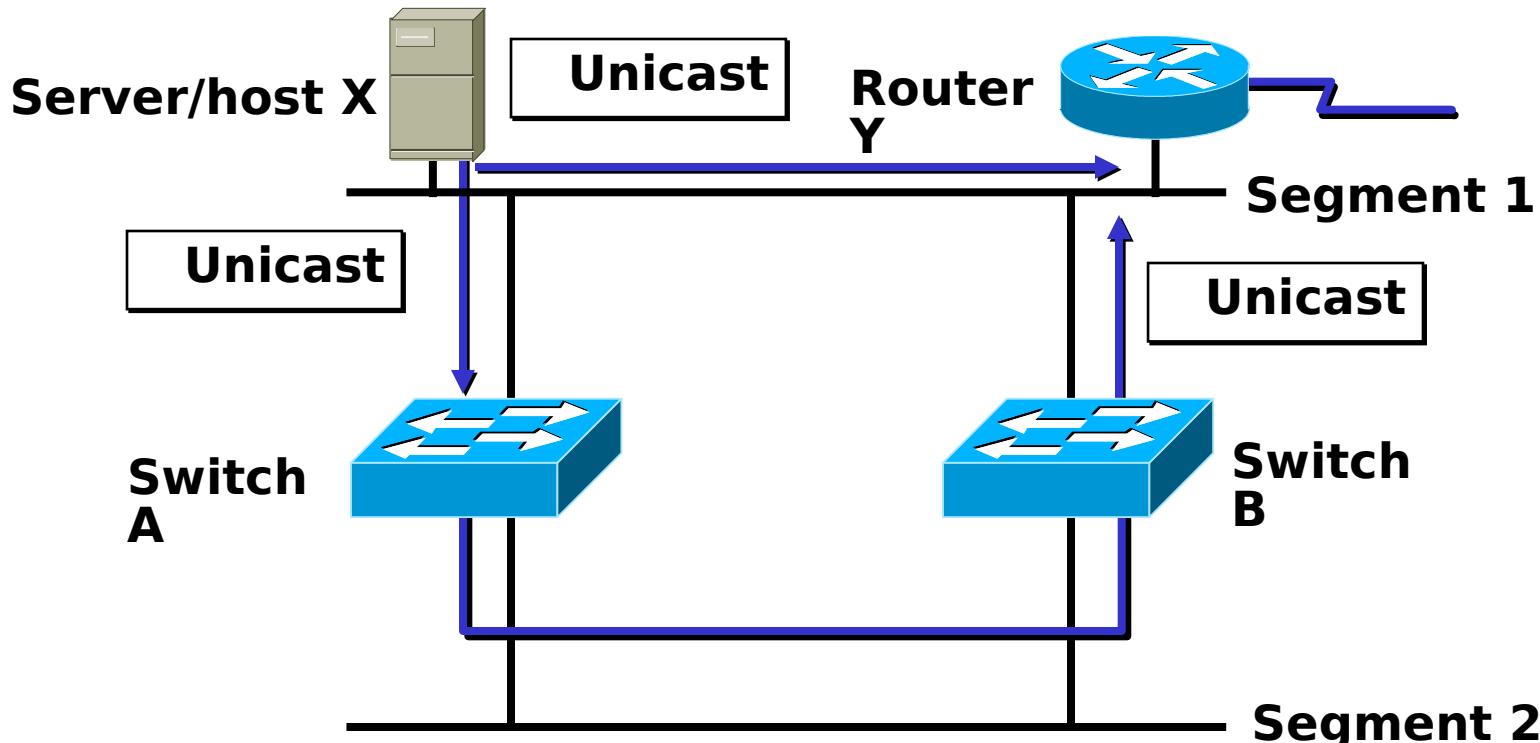
Multiple Frame Copies



- Host X sends an unicast frame to router Y
- Router Y MAC address has not been learned by either switch yet

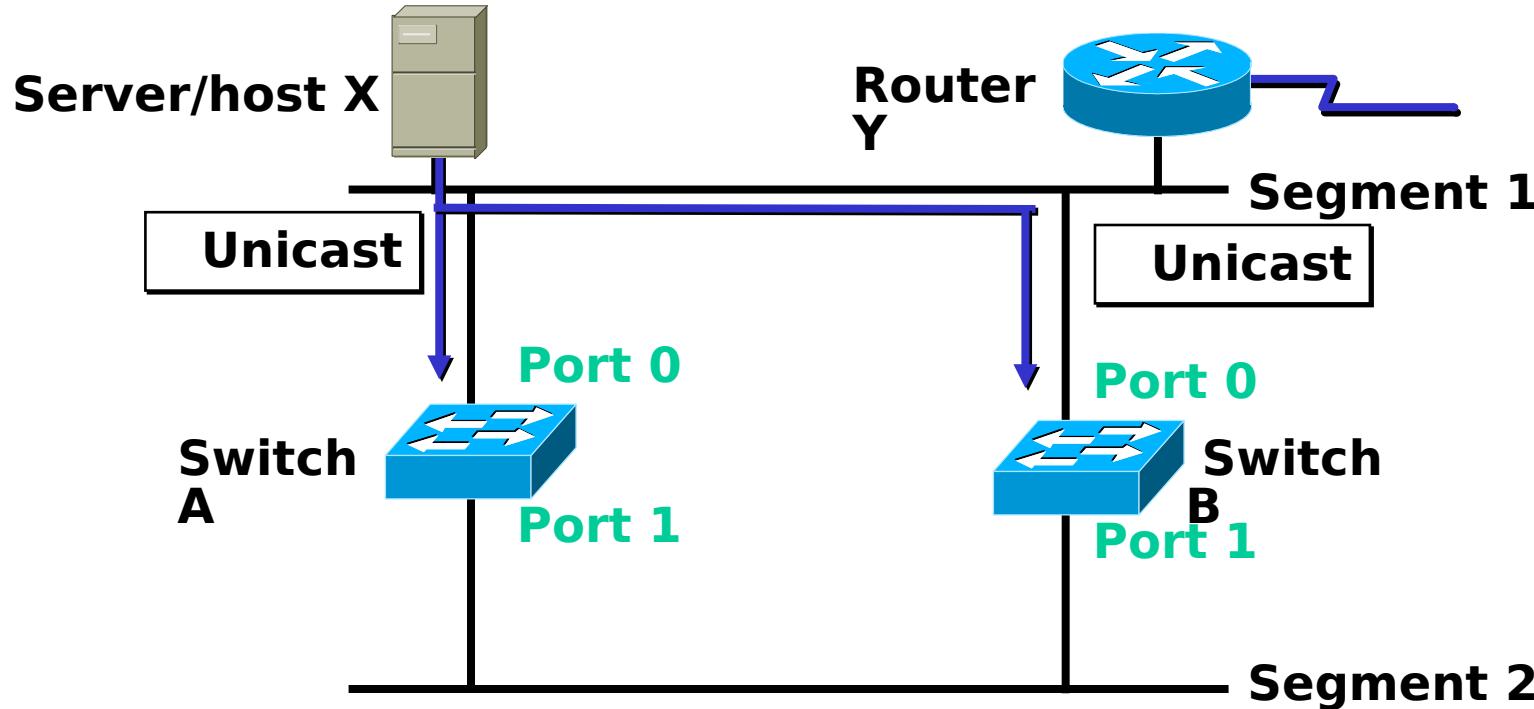
Multiple Frame Copies

MSTP



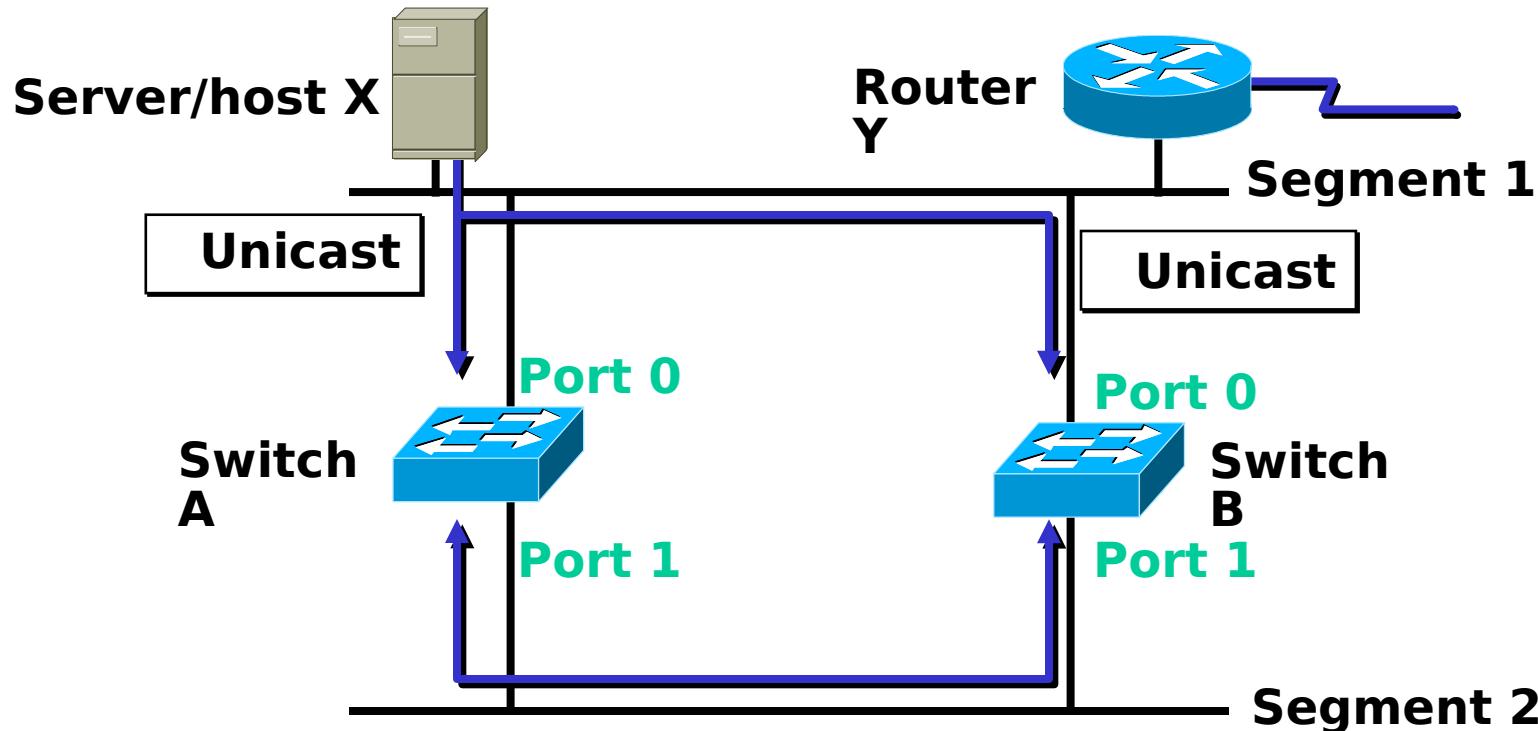
- Host X sends a unicast frame to Router Y
- Router Y MAC Address has not been learned by either Switch yet
- Router Y will receive two copies of the same frame

MAC Database Instability



- Host X sends an unicast frame to Router Y
- Router Y MAC Address has not been learned by either Switch yet
- Switch A and B learn Host X MAC address on port 0

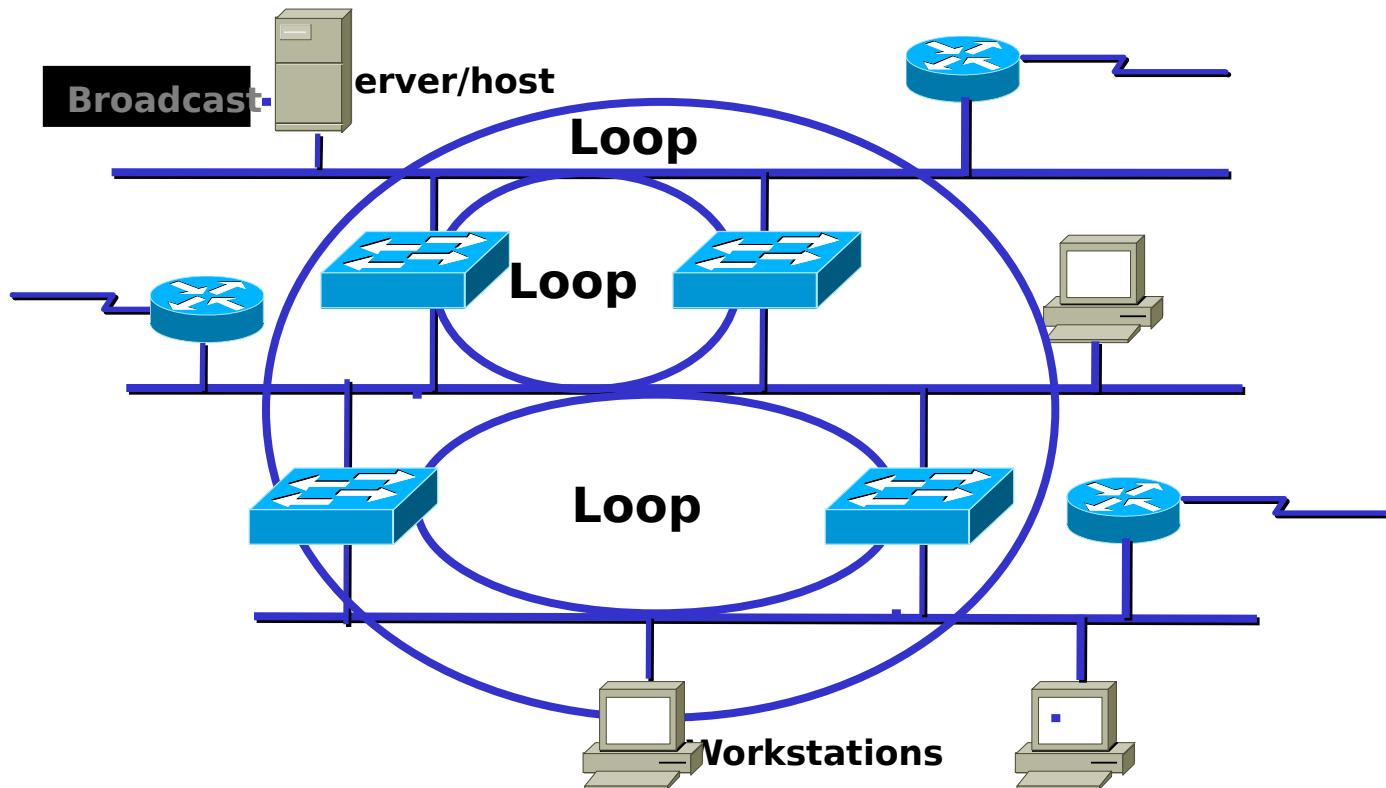
MAC Database Instability



- Host X sends an unicast frame to Router Y
- Router Y MAC Address has not been learned by either Switch y
- Switch A and B learn Host X MAC address on port 0
- Frame to Router Y is flooded
- Switch A and B incorrectly learn Host X MAC address on port 1

Multiple Loop Problems

MSTP

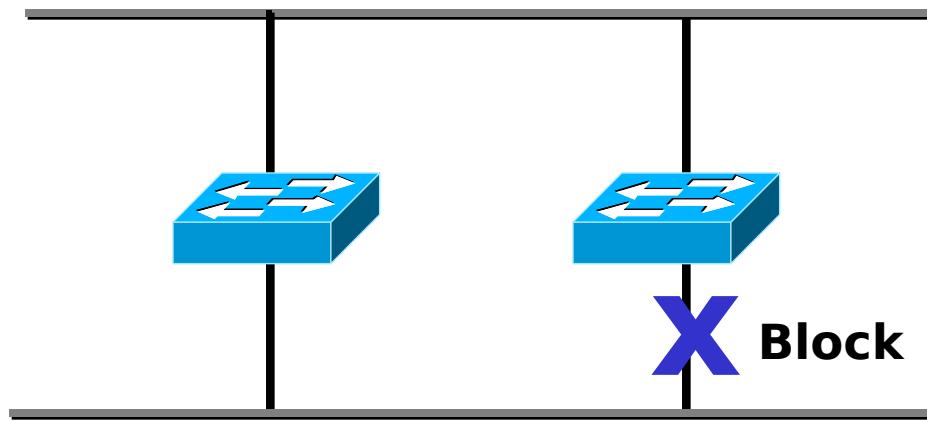


- Complex topology can cause multiple loops to occur
- Layer 2 has no mechanism to stop the loop

Solution: Spanning-Tree Protocol



MSTP



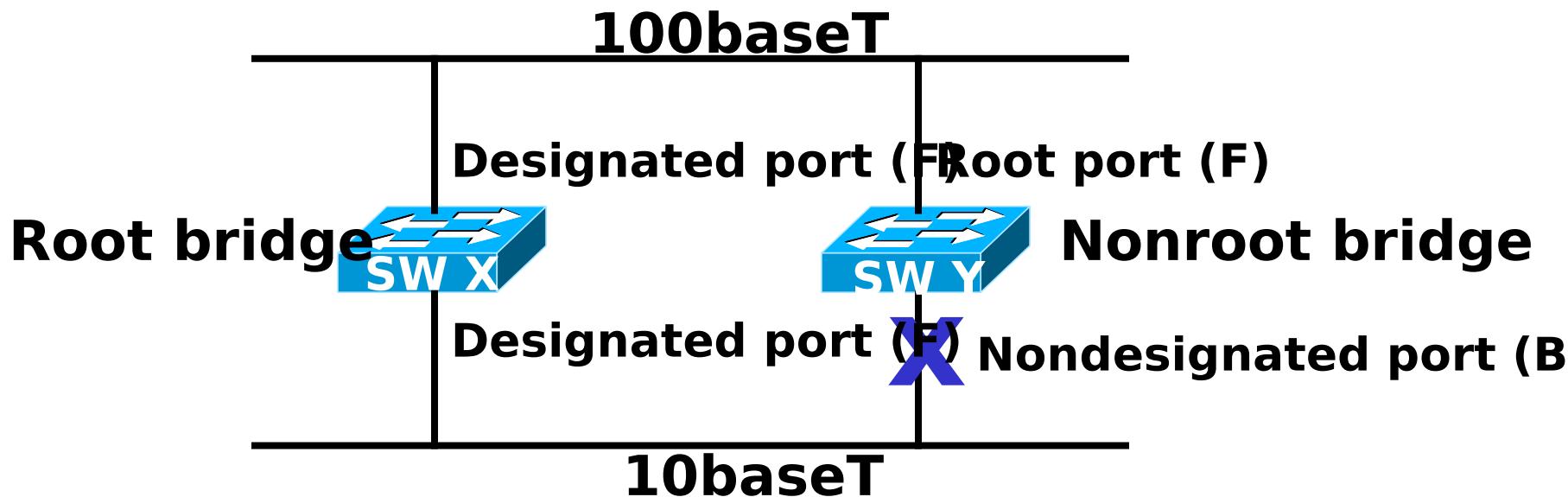
Provides a loop free redundant network topology placing certain ports in the blocking state



Spanning-Tree Operations

MSTP

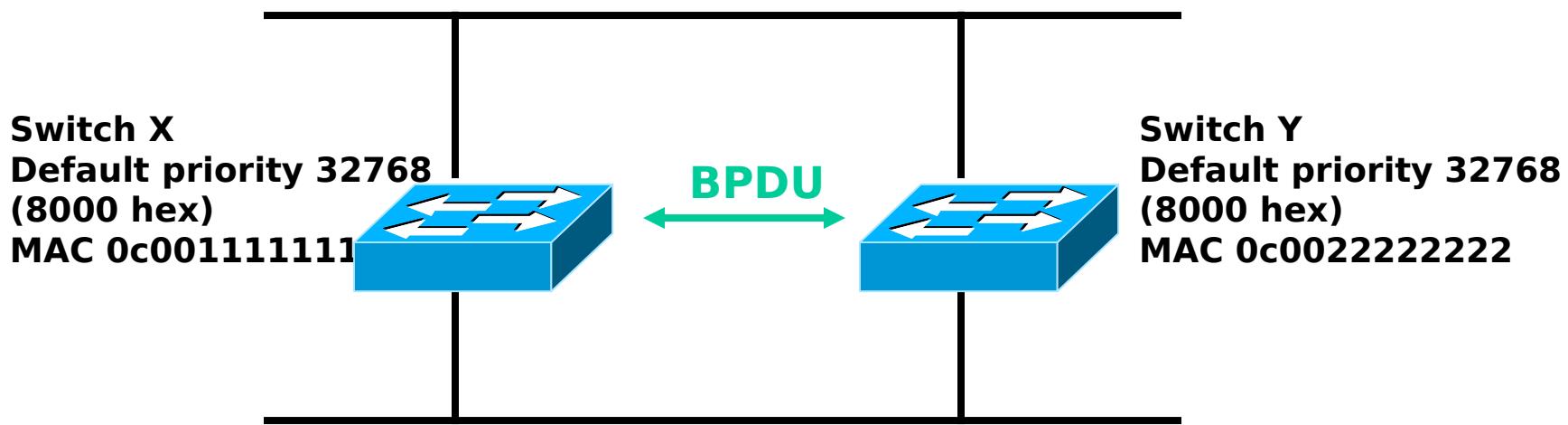
- One root bridge per network
- One root port per nonroot bridge
- One designated port per segment





Root Bridge Selection

MSTP



**BPDU = Bridge protocol data unit
(default = sent every 2 seconds)**

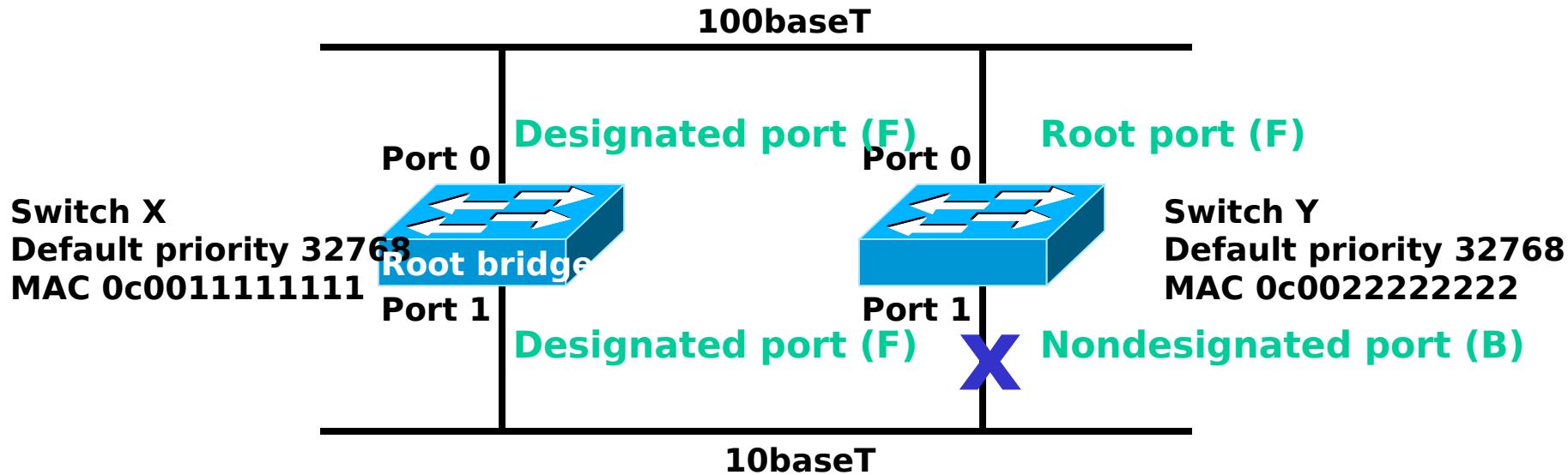
Root bridge = Bridge with the lowest bridge ID

Bridge ID = Bridge priority + bridge MAC address

In the example, which switch has the lowest bridge ID?

Port States

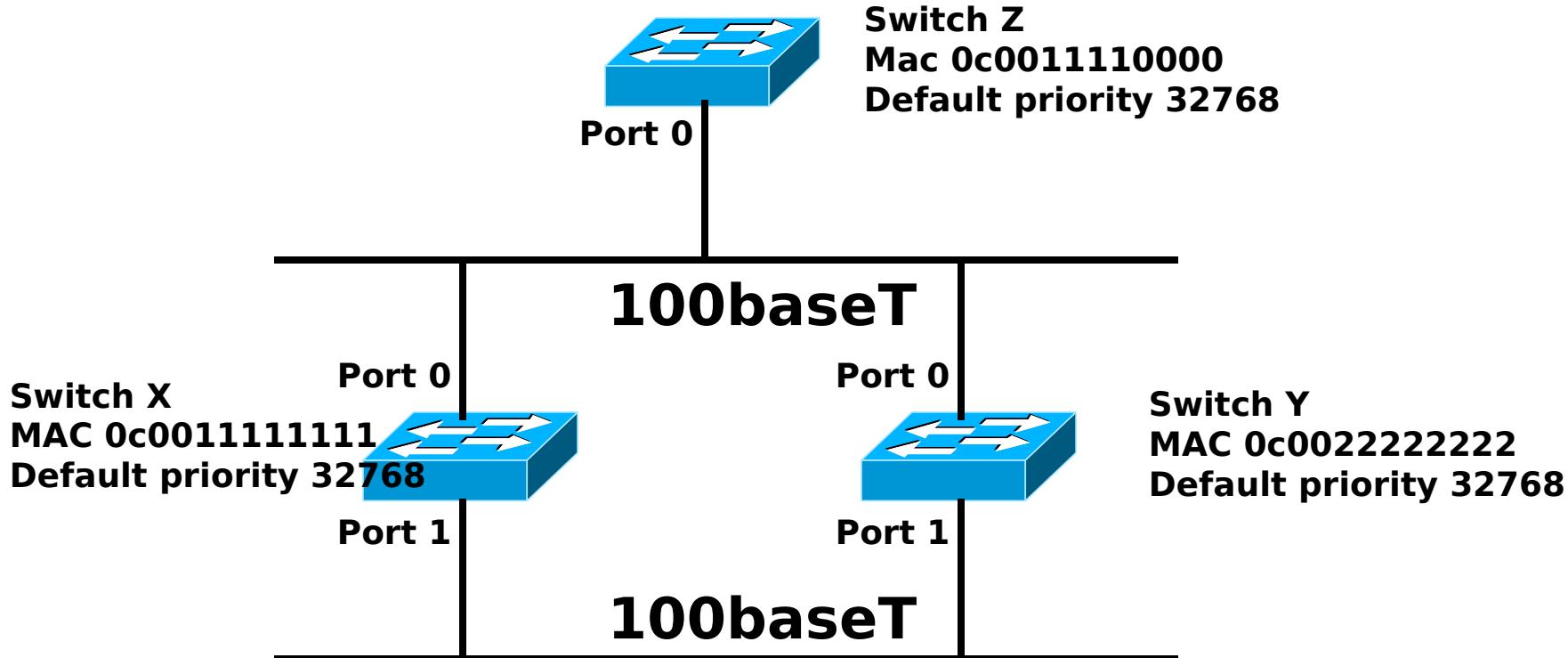
MSTP





Spanning-Tree

MSTP



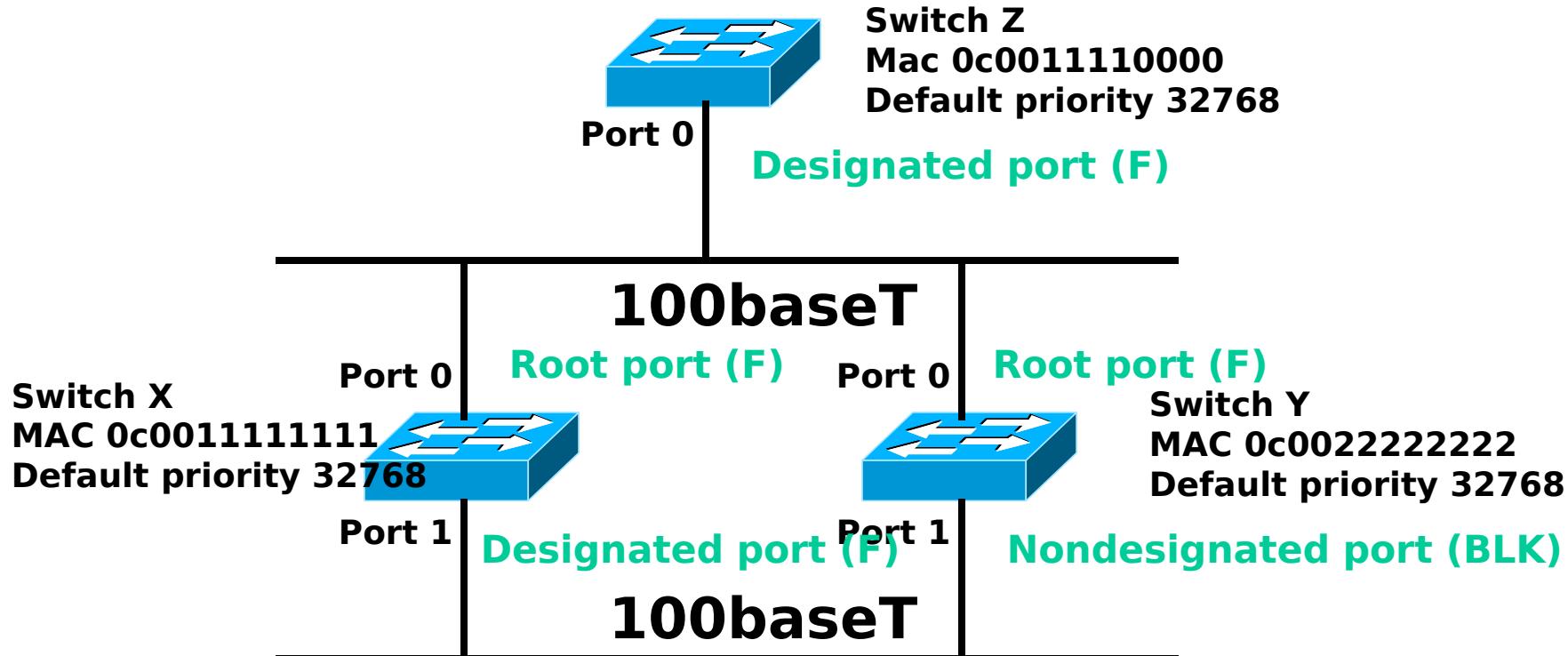
Can you figure out:

- What is the root bridge?
- What are the designated, nondesignated, and root parts?
- Which are the forwarding and blocking ports?



Spanning-Tree

MSTP



Can you figure out:

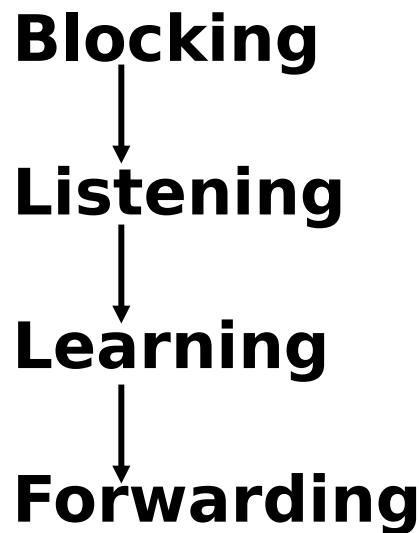
- What is the root bridge?
- What are the designated, nondesignated, and root parts?
- Which are the forwarding and blocking ports?



Spanning-Tree Port States

MSTP

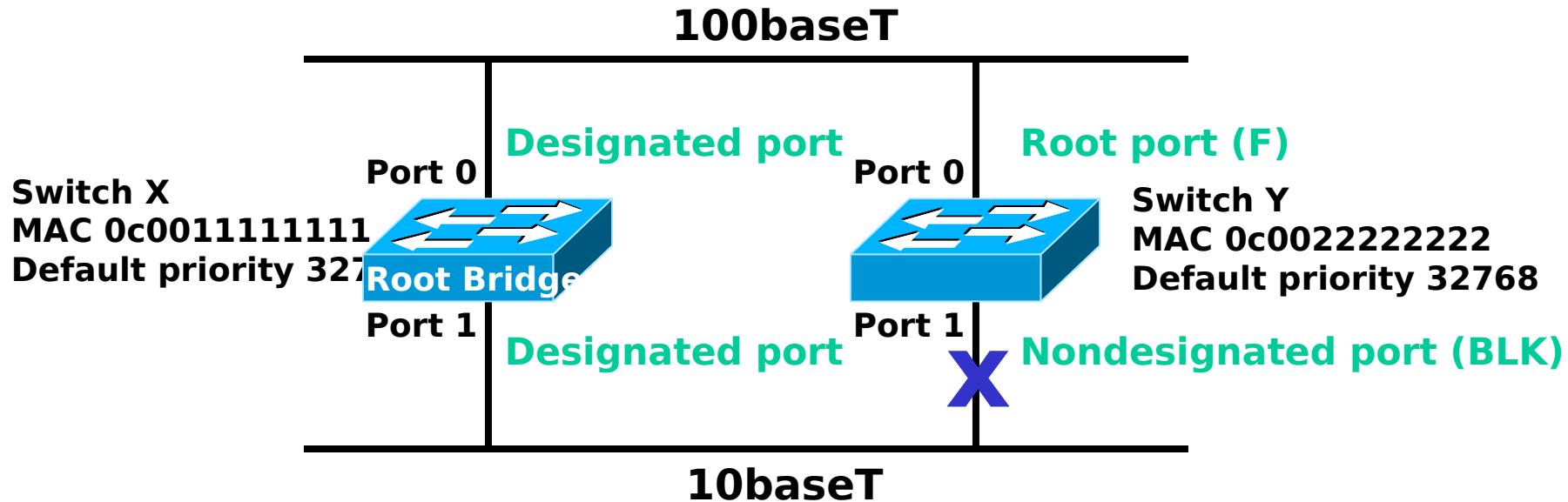
Spanning-tree transitions each port through several different state:





Spanning-Tree Recalculation

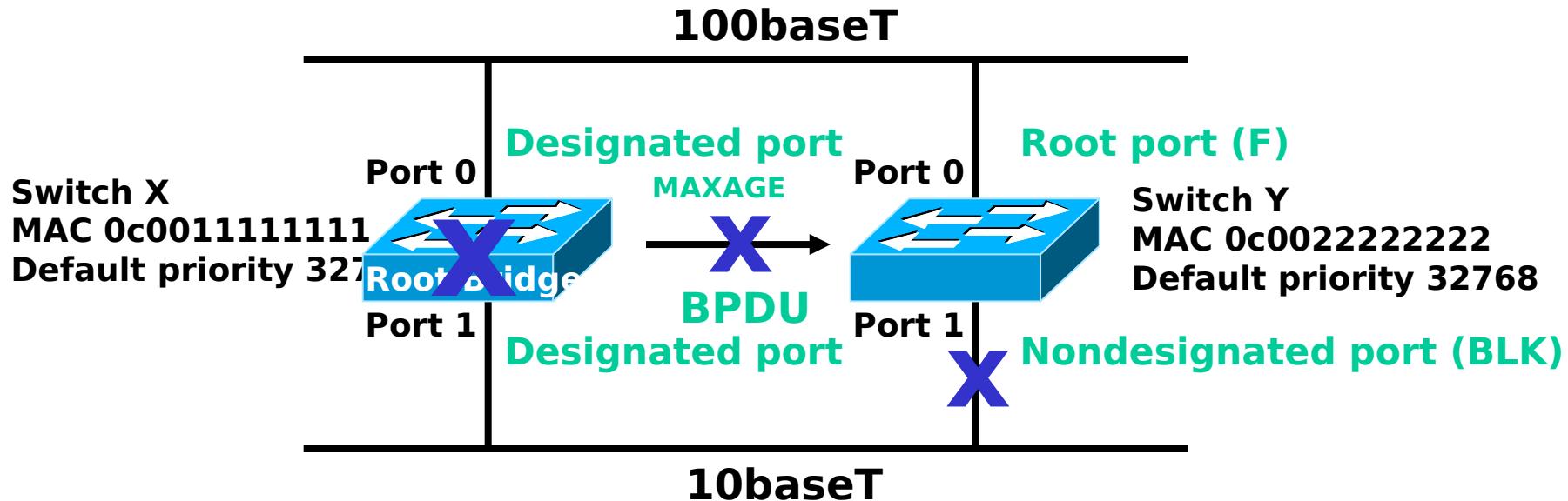
MSTP





Spanning-Tree Recalculation

MSTP





Key Issue:

MSTP

Time To Convergence

- **Convergence occurs when all the switches and bridge ports have transitioned to either the forwarding or blocking state**
- **When network topology changes, switches and bridges must recompute the Spanning-Tree Protocol, which disrupts user traffic**



Planning Considerations

MSTP

- Identify Port Assignments
 - Identify a policy of trunk port placement
 - Identify placement of root switch
- Plan for expansion
 - Never plan to use full port density on a switch

Any Questions?

